inera

# Anvisning för informationsklassificering

2018-12-13

Version 2.3

inera

| Revisionshistorik | | |
|---|---|---|
| **Version** | **Författare** | **Kommentar** |
| 1.9 | Fredrik Rosenberg | Uppdatering av äldre version |
| 2.0 | Fredrik Rosenberg | Beslutad av Sara Meunier, chef Arkitektur och regelverk, Inera |
| 2.1 | Fredrik Rosenberg | Redaktionella ändringar |
| 2.2 | Fredrik Rosenberg | Tillägg om aspekten Spårbarhet |
| 2.3 | Fredrik Rosenberg | Harmonisering till Myndigheten för samhällsskydd och beredskap samt SKL gällande benämningar |

| Referenser | | |
|---|---|---|
| R1 | QLIS - Riktlinje och kvalitetsmanual<br><br>Integrerat ledningssystem för Kvalitet och Informationssäkerhet. | https://intra.inera.se/Documents/Policies_o_riktlinjer/riktlinje_kvalitetsmanual.pdf?epslanguage=sv |

# Innehåll

# Om informationsklassificering

Information är en viktig tillgång för Inera. Inera ska identifiera skyddsvärd information och därefter vidta rimliga och väl avvägda skyddsåtgärder. Enligt Ineras riktlinjer för kvalitet och informationssäkerhet, QLIS, ska alla viktiga informationstillgångar inom Inera klassificeras.

Informationsklassificering är en process som syftar till att kategorisera den information som Inera hanterar. Klassificeringen blir ett sätt att dela in olika typer av information bland annat baserat på hur viktig informationen är för Ineras verksamhet.

Klassificeringen som tas fram är även ett underlag som ligger till grund för fortsatt arbete med riskanalyser, krav på IT-säkerhet, fysiskt skydd, hanteringsrutiner och kontinuitetshantering.

Anvisningen gäller för all hantering av information inom Inera oavsett var eller i vilken form hanteringen sker.

# Ansvar för att klassificering sker

Det är primärt den som ansvarar för tjänsten som är ansvarig för att informationsklassificering sker. Om en speciellt utpekad ansvarig inte finns gällande informationsmängden är det enhetschef som är ansvarig. Företrädesvis tas hjälp av företrädare för den verksamhet som använder tjänstens komponenter, i de fall det är oklart hur klassificeringen ska ske. Exempelvis om olika verksamheter har olika behov av samma information och därmed bedömer att den tillhör olika informationsklasser. Klassificeringen ska dokumenteras med hjälp av mall och ska kunna återfinnas via förvaltningsplanen. Rådande version av klassificeringen ska även skickas till den som ansvarar för informationssäkerheten på Inera. Mall för dokumentation återfinns i slutet av denna riktlinje.

Informationsklassificering ska genomföras/uppdateras:

- vid etablering eller införande av ett nya IT-stöd
- när ny informationsmängder/informationstyper tillförs
- vid större ändringar av rutiner som påverkar informationshanteringen
- när externa krav på informationshanteringen förändras
- inför upphandling och utveckling av IT-system/tjänst
- inför outsourcing

inera

# IT-system och informationsklassificering

IT-systemet anses, vid framtagande av säkerhetsåtgärder, tillhöra samma klass som den information det innehåller. Vid olika klassificering av ingående information gäller den högsta klassen. Säkerhetskrav för IT-systemet ska baseras på den tilldelade klassificeringsnivån.

Syftet med att föra över informationens klassificering till behandlande IT-system är att man kan koppla IT-säkerhetsåtgärder mot tilldelad klass.

I mallen för informationsklassificeringen anges vilka IT-stöd/IT-komponenter som hanterar informationen.

# Information med bäring på rikets säkerhet

En liten del av den information som hanteras inom landsting, regioner, kommuner och privata vårdgivare har bäring på rikets säkerhet, och kan därmed omfattas av Säkerhetsskyddslagen och vissa delar av Offentlighets- och sekretesslagen. Inera skulle därmed, potentiellt kunna hamna i ett läge där denna information hanteras. Anvisningen syftar dock inte till att identifiera denna typ av information. Om misstanke finns att informationen kan ha bäring på rikets säkerhet görs separat utredning om detta med stöd av jurist.

# NMI-klassificering

I vissa fall kan klassificeringen av information indikera påverkan på och konsekvenser för patients liv och hälsa. I så fall kan det IT-system som hanterar informationen omfattas av Läkemedelsverkets föreskrifter (LVFS 2014:7) och klassas som ett NMI (Nationellt Medicinskt Informationssystem). För att avgöra detta skall Ineras metod för NMI-klassificering användas.

inera

# Genomförande

## Informationsklassificering

1. Definiera vilka informationsmängder som ska informationsklassificeras samt vilka IT-system som hanterar informationen. Om informationsklassificering inte gjorts tidigare kan det vara lättast att börja med ett bredare omfång, till exempel all information i ett IT-stöd.

2. Identifiera tjänster/verksamheter/processer som informationen ingår i. Detta för att lättare kunna bedöma konsekvensnivåer i klassificeringen. Hur informationen används och i vilket syfte har stor betydelse för klassificeringen.

3. Utse en arbetsgrupp som ska klassificera informationen. Det är viktigt att det finns representanter för fler informationsägare i de fall flera olika använder informationen. Framför allt är det viktigt att ha representation från de som kan förväntas ha det största behovet.

4. Genomför klassificeringen och dokumentera resultatet. Varje informationsmängd ska bedömas utifrån vad konsekvensen blir vid bortfall av någon av aspekterna:

   - Konfidentialitet – att informationen endast är åtkomlig för behöriga personer
   - Riktighet – att informationen är korrekt och fullständig
   - Tillgänglighet – att informationen finns tillgänglig för behöriga när de behöver den

   Kommentar: Aspekten Spårbarhet klassas inte separat utan bedöms i stället som en skyddsåtgärd baserad på informationens konfidentialitetsklass.

   Bedömningen görs sedan utifrån konsekvensnivåerna:

   Nivå 3 – Allvarlig (röd),

   Nivå 2 – Betydande (orange)

   Nivå 1 – Måttlig (gul)

   Nivå 0 – Försumbar (grön).

   För stöd gällande hur bedömningen ska ske, se Bilaga 1: Bedömningsgrunder.

inera

# Frågor som stöd vid en informationsklassificering

**Konfidentialitet**

Vad blir konsekvensen om någon obehörig får tillgång till informationen?

Vad händer om media får tillgång till informationen?

**Riktighet**

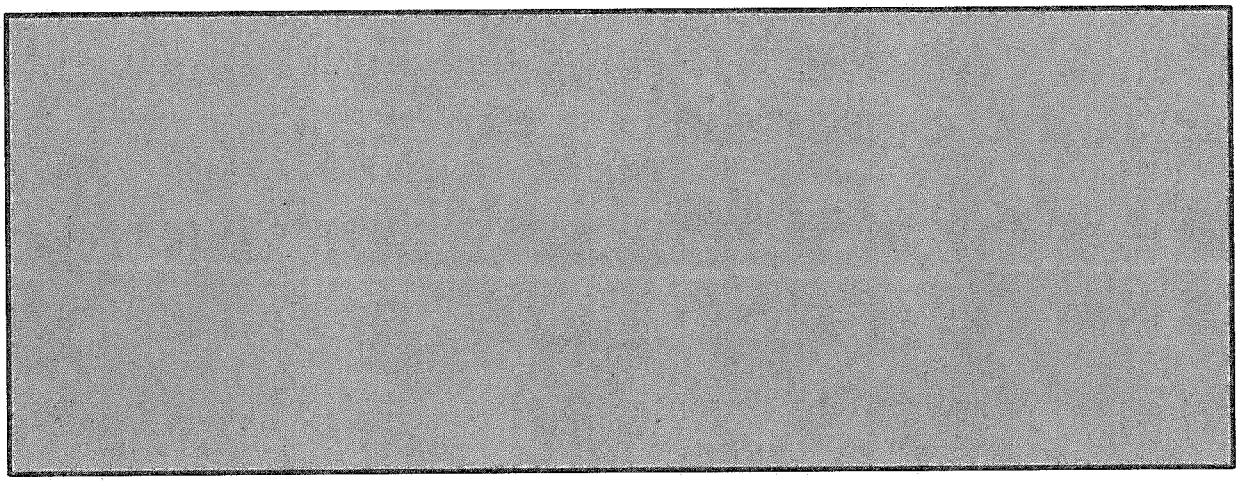
Vad blir konsekvensen om obehörig person eller process förändrar informationen?

Vad blir konsekvensen om verksamheten inte upptäcker detta?

**Tillgänglighet**

Vilken konsekvens får det om informationen inte alls kan användas på grund av bortfall av tillgänglighet?

Vilken konsekvens får det om informationen kan användas, men endast i begränsad utsträckning?



inera

# Bilaga 1: Bedömningsgrunder

## Bedömning av konsekvens

| Nivå | Konsekvens | Perspektiv och exempel |
|---|---|---|
| 3 | **Allvarlig** | **Person/Invånare/Medarbetare**<br>Mycket stor påverkan på liv, hälsa, rättigheter (allvarlig fysisk- eller integritetsskada och/eller dödsfall).<br>**Kunder**<br>Mycket stor negativ effekt på kunders förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.<br>Till exempel:<br>• Stoppar kritiska e-hälsotjänster mer än 4 tim. dagtid<br>• Vårdens/omsorgens krisorganisation initieras<br>**Inera/Projekt**<br>Mycket stor negativ effekt på Ineras förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.<br>Till exempel:<br>• Mycket stora direkta eller indirekta skadekostnader – mer än 10 mkr<br>• Ineras krisorganisation initieras<br>**Förtroendeskada**<br>Ineras och/eller e-hälsans varumärke skadas allvarligt. Myndighetsfråga. Troliga politiska konsekvenser.<br>Till exempel:<br>• Omfattande negativ publicitet i riksmedia<br>• Nationell kundtjänst överbelastad |
| 2 | **Betydande** | **Person/Invånare/Medarbetare**<br>Stor påverkan på liv, hälsa, rättigheter (fysisk- eller integritetsskada och/eller dödsfall).<br>**Kunder**<br>Stor negativ effekt på kunders förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.<br>Till exempel:<br>• Stoppar flertalet e-hälsotjänster mellan 15 min och 4 tim<br>**Inera/Projekt**<br>Stora direkta eller indirekta skadekostnader.<br>Till exempel:<br>• 1 mkr till 10 mkr<br>**Förtroendeskada**<br>Ineras anseende ifrågasätts och e-hälsans eller Ineras varumärke skadas. Styrelsefråga.<br>Till exempel:<br>• Negativ publicitet i riksmedia<br>• Omfattande klagomål inkommer |

| | | |
|---|---|---|
| 1 | **Måttlig** | **Person/Invånare/Medarbetare**<br>Patient/Person riskerar att lida fysisk skada eller integritetsskada<br>**Kunder**<br>Måttlig negativ effekt på kunders förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.<br>**Inera/Projekt**<br>Viss direkt eller indirekt skadekostnad.<br>Till exempel:<br>• 100 tkr till 1 mkr<br>**Förtroendeskada**<br>Måttlig förtroendeskada.<br>Till exempel:<br>• Negativ publicitet i lokala media. Vd-fråga<br>• Klagomål inkommer |
| 0 | **Försumbar** | **Person/Invånare/Medarbetare**<br>Mycket liten eller ingen påverkan på patient/person<br>**Kunder**<br>Försumbar påverkan på kunders verksamhet.<br>Till exempel:<br>• Ingen stoppande påverkan på e-hälsotjänster<br>**Inera/Projekt**<br>Ingen märkbar skadekostnad.<br>Till exempel:<br>• < 100 tkr<br>**Förtroendeskada**<br>Försumbar förtroendeskada.<br>Till exempel:<br>• Tas upp som fråga i Ineras förvaltningsorganisation<br>• Enstaka klagomål inkommer |

**Kommentar:** Om konsekvensen enligt ovan bedöms vara ***Allvarlig*** **(3)** ur ett invånarperspektiv men endast måttlig ur ett ekonomiskt perspektiv blir den sammanlagda bedömningen av konsekvensen ändå ***Allvarlig*** **(3)**

inera

## Exempel på information i de olika klasserna

| Nivå | Konfidentialitet[1] | Riktighet[2] | Tillgänglighet[3] |
|---|---|---|---|
| 3 | *Information med mycket högt skyddsvärde* | *Information där riktigheten aldrig ska kunna gå att ifrågasättas. Det ska inte gå att göra fel.* | *Information som ska finnas tillgänglig inom mindre än15 minuter, dygnet runt* |
| 2 | *Skyddsvärd information av högre känslighet som kräver att åtkomst begränsas. T ex sekretessbelagda personuppgifter* | *Information som kräver att skyddet för riktighet är högt och att avsevärd vikt läggs på att upprätthålla riktigheten* | *Information som ska finnas tillgänglig inom två timmar* |
| 1 | *Information där visst behov finns att kunna begränsa åtkomsten.* | *Information där riktigheten ska finnas men som inte kräver mer än periodvisa kontroller* | *Information som bör finnas tillgänglig på dagtid inom ett antal timmar* |
| 0 | *Ej känslig information* | *Information som inte i efterhand kräver kontroll av om den förändrats* | *Informationen som bör finnas tillgänglig inom ett antal dagar* |

[1] Exempel på åtgärder för att upprätthålla Konfidentialitet är: Behörighetsstyrning, stark autentisering, loggning eller kryptering
[2] Exempel på åtgärder för att upprätthålla Riktighet är: Digitala signaturer, manuella signaturer, formatkontroll vid inmatning eller rimlighetsbedömningar av inkommen data
[3] Exempel på åtgärder för att upprätthålla Tillgänglighet: Dubblerade driftsmiljöer, redundans i nätverk, SLA-krav på leverantörer eller noggranna testprocesser

# Bilaga 2: Mall för dokumentation av genomförd klassificering

Resultat av informationsklassificering för:_____

| Nr | Informationsmängd | Beskrivning | Konf | Rikt | Tillg |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| 9 | | | | | |
| 10 | | | | | |

Berörda IT-system samt högsta klassificering för informationen som hanteras

| It-system/It-komponenter | Beskrivning eller kommentar | Konf | Rikt | Tillg |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Mall för ifyllnad finns att hitta bland Ineras övriga mallar.