Informationsklassning och säkerhetsnivåer

# Vem informationsklassar

Informationssäkerhetssamordnare (ISSO) identifierar behov av klassning och tar med ärendet till *Nätverk informationssäkerhet* som tar fram förslag till säkerhetsnivå. ISSO genomför klassningen efter samråd med verksamhetsansvariga/funktionsansvariga. Behov av ny klassning eller komplettering av klassning baseras på ny eller förändrad information, till exempel i form av lagar och föreskrifter.

## Vem beslutar

Nätverkets förslag på säkerhetsnivå förankras, genom informationssäkerhetssamordarens försorg, i respektive förvaltning. Därefter fastställs dokumentet av regional säkerhetsansvarig på Regionkontoret.

# Informationsklassningsprocess

|  |  |
| --- | --- |
|  | Information som hanteras |
| Identifiera typ av information | Information identifieras för att få kunskap om innehållet, och avgöra behov av klassning.  |
| Fastställa kritiska system/funktioner/tillgänglighet | Objektsfamilj enligt förvaltningsmodell pm3 fastställer vilka system som är verksamhets-kritiska. Dessa system/funktioner har krav på hög tillgänglighet och hög servicenivå. System och servicenivåer finns beskrivna i regionens gemensamma applikationslista på intranätet. |
| Genomföra klassning av informationen enligt rutin | Metod för klassning av information framgår av rutin *Informationsklassning*. Klassning dokumenteras på blankett *Protokoll informationsklassning*. Vid ny typ av information eller förändringar genomförs ny klassning. Konsekvensbedömning och värdering av var, hur och när information kan förloras, förvanskas, omhändertas av obehöriga med mera. |
| Fastställa säkerhetsnivå | Som resultat av informationsklassningen bestäms säkerhetsnivå. De partner/intressenter som ska säkra skyddsnivån kontaktas för information och säkerställande av önskemål/krav. |
| Klarlägga hanteringen | Hur klassad elektronisk information och information på papper, band, film med mera ska hanteras framgår i kapitel 309 Informationssäkerhet. |
|  | Information ska vara skyddad enligt lagar, andra krav och egna beslut. |

# Information/handlingar som informationssäkerhetsklassas

|  |  |
| --- | --- |
| **Personalhandlingar** | **Säkerhetsnivå** |
| Anställningsbevis | Grund |
| Avslut av anställning | Grund |
| Beslut från försäkringskassan | Mycket hög |
| Beslut om jämkning | Hög |
| Beslut om utmätning | Mycket hög |
| Betyg/intyg | Hög |
| Brev till personal med känslig information(hat/hot) | Mycket hög |
| Domar  | Mycket hög |
| Enskild överenskommelse | Hög |
| Läkarintyg (personalavdelning) | Mycket hög |
| Lönebeslut/Förhandlingsprotokoll | Hög |
| Omplaceringar | Mycket hög |
| Pensionshandlingar | Mycket hög |
| Polisanmälan | Mycket hög |
| Registerutdrag SÄPO | Mycket hög |
| Rehabiliteringsutredningar | Mycket hög |
| Tjänstbarhetsintyg | Hög |
| Tjänstelegitimation (SITHS-kort) – underlag, foto, reservkort m m | Mycket hög |
| Underlag för löneberäkning | Grund |
| Utvecklingssamtal (utvecklings-, ledar- och avgångssamtal) | Mycket hög |
| Varning (personalavdelning) | Mycket hög |

|  |  |
| --- | --- |
| **Ekonomihandlingar** | **Säkerhetsnivå** |
| Bokföring Fakturor | Hög |
| Budget/Bokslut | Grund |
| Donationer – ansökningar/beslut | Hög |

|  |  |
| --- | --- |
| **Politiska handlingar** | **Säkerhetsnivå** |
| Mål | Hög |
| Policy och riktlinjer | Hög |
| Protokoll | Hög |
| Rapporter/planer | Hög |
| Reglementen | Hög |
| Utredningar | Hög |
| Övriga styrdokument | Hög |

|  |  |
| --- | --- |
| **Administrativa handlingar** | **Säkerhetsnivå** |
| Avtal | Hög |
| Avvikelse vara/tjänst/händelse, klagomål | Grund |
| Bygg- och installationsritningar | Mycket hög |
| E-post | Grund |
| Hemlig handling enligt säkerhetsskyddslagen 2018:585 | Mycket hög \* |
| Händelseanalys | Hög |
| Händelselogg TiB | Mycket hög |
| Information på Intranät | Grund |
| Information på www.regionhalland.se | Grund |
| Informationsklassning rutin och resultat | Grund |
| Informationsklassningsprotokoll | Hög |
| It-behörigheter beslut | Hög |
| Kalibreringsintyg | Mycket hög |
| Krisdagbok | Mycket hög |
| Kryptohandlingar (krypteringssalt) | Mycket hög |
| Ledningssystemet grunddokumentation | Grund |
| Licenser – it | Hög |
| Lösenordsförteckning IT Service | Mycket hög |
| Minnesanteckningar / mötesanteckningar | Grund |
| Planer/Protokoll/Projekt | Grund |
| Dataskyddsförordningen – register – anmälan och förteckning | Grund |
| Dataskyddsförordningen -Personuppgiftsbiträdesavtal | Hög |
| Resultat av loggkontroller | Mycket hög |
| Revision extern iakttagelserapport/plan för korrigerande åtgärder.Klassas i varje enskilt fall. | Lägst hög |
| Revisionsrapporter/uppdrag | Grund |
| Risk- och sårbarhetsanalyser resultat (utförs på initiativ av och medmedverkan av regionens säkerhetssamordnare på Regionkontoret) | Mycket hög |
| Riskanalyser resultat enligt olika fastställda metoder i ledningssystemet avsnitt 4, kapitel 406.*Resultat riskanalyser/händelseanalyser - protokoll - (lägst h, varje riskanalysresultat måste klassas för sig)* *Ansvarig: Analysledare* *Riskanalyser - handlingsplaner**(lägst h, varje riskanalys - handlingsprogram måste klassas för sig) Ansvarig: Handlingsplansansvarig*  | Lägst hög |
| Rutiner/Manualer | Grund |
| Systemdokumentation – teknisk beskrivning | Mycket hög |
| Systeminformation – verksamhetsbeskrivning/manualer/handböcker | Grund |
| Säkerhetskopior | Mycket hög |
| Trycksaker | Grund |
| Upphandlingsunderlag | Mycket hög |
| Uttalande om tillämplighet | Hög |
| Verksamhetsplan/verksamhetsberättelse/balanserat styrkort | Hög |
| Viktningssammanställning IT-system | Hög |

|  |  |
| --- | --- |
| **Patienthandlingar och handlingar som har betydelse för vård** | **Säkerhetsnivå** |
| Analyser | Hög |
| Bårhusliggare/information om avliden | Hög |
| Forskningsrapporter | Hög |
| Händelseanalys patient | Mycket hög |
| Information från medicintekniska produkter | Mycket hög |
| Lex Maria – anmälan/beslut | Mycket hög |
| Operationsplanering | Mycket hög |
| Patientadministration | Hög |
| Patientavvikelser | Mycket hög |
| Patientjournaler/handlingar | Mycket hög |
| Patientjournalsystem, loggar | Mycket hög |
| Patientnämndsadministration | Mycket hög |
| Tidbok | Hög |
| Vård och handläggningsöverenskommelser | Hög |
| Vårdriktlinjer | Hög |

|  |  |
| --- | --- |
| **Skolrelaterade handlingar**  | **Säkerhetsnivå** |
| Pedagogiskt material:Elevarbeten, lektionsplaneringar, | Grund |
| Betyg (elever) | Hög |
| Omdömen | Hög |
| Elevakter (skolsköterska) och utredningar (kurator, specialpedagoger, psykologiska utredningar och disciplinära utredningar). | Mycket hög |
| Elevvårdskonferens, åtgärdsprogram och antimobbinggruppen | Hög |
| Individuell utvecklingsplan (allmän handling) | Grund |
| Digitala elevadministrativa (Dexter, Extens, It´s learning, Skola 24) handlingar: (val av program, kurser, hemadress, telefonnummer, vårdnadshavare med mera). | Grund |
| Elevadministrativa handlingar/akter (i papper) T.ex. Samlad akt från tidigare skolor men även allt samlat från gymnasietiden | Hög |
| Verksamhetsdokument: T.ex. djurhållningsdokument, miljöronder mm. | Grund |

\* Säkerhetsskyddade uppgifter hanteras i särskilt ordning.

# Styrning av informationssäkerheten



Hanteringen av information är styrd av lagar, föreskrifter och egna beslut. I verksamheten hanteras information på olika media och via olika kommunikations-kanaler. Informationsklassning genomförs enligt särskild rutin och uppdateras vid behov. Den praktiska hanteringen styrs utifrån informationsklassningen. I kapitel *309* beskrivs hur information ska hanteras. Styrningen av informationsklassningen ska säkra att hanteringen upplevs som säker, tillräcklig och förebyggande.

Informationsklassningens syfte är att bedöma informationens värde och känslighet utifrån olika krav. Bedömningen leder till en klassning som avgör säkerhetsnivån för informationen och/eller informationssystemet. Resultatet blir ett underlag för hur information får hanteras i verksamheten och i it-system. Utifrån resultatet av klassningen ansvarar informationsägaren (verksamhetschef/motsvarande) och enligt pm3-modellen respektive objektägare/objektägare it. för hanteringen av information i verksamheten respektive i it-system.

## Rutin

ISSO använder Rutin [*Informationsklassning* *för informationssäkerhetssamordnare* (ISSO)](https://rh.sharepoint.com/sites/Informationssakerhet_och_sakerhet/ODMPublished/RH-9721/Informationsklassning%20f%C3%B6r%20informationss%C3%A4kerhetssamordnare.docx) som finns på nätverkets samarbetsplats.

## Protokoll

Informationsklassningen dokumenteras i ett protokoll som förvaras hos ISSO.

# Säkerhetsnivåer

Resultat av informationsklassningen är att säkerhetsnivåer bestämts.

Dessa nivåer är:

* Grundnivå (g) lindriga risker/konsekvenser - innebär att informationen inte kräver något extra skydd.
* Hög nivå (h) allvarliga risker/konsekvenser - innebär att informationen ska vara under direkt uppsikt eller inlåst.
* Mycket hög nivå (m) mycket allvarliga risker/konsekvenser - innebär att informationen ska vara under direkt uppsikt eller inlåst i brandklassat skåp eller motsvarande.

## Resultat av Riskanalyser/Händelseanalyser

Resultat av riskanalys och handlingsplan efter riskanalys ska klassas i varje enskilt fall. Detsamma gäller för händelseanalyser. Händelseanalyser patient ska alltid klassas med mycket hög säkerhet. Säkerhetsnivå ska anges i protokoll och handlingsplan. För råd och hjälp kontakta informationssäkerhetssamordnaren (ISSO).

## Externa revisionshandlingar

Externa revisionshandlingar klassas i varje enskilt fall

## It-system

It-system kan innehålla information med olika säkerhetsnivåer. It-system klassas utifrån den information i systemet som har den högsta säkerhetsnivån och görs av personal på IT Service.

## Information som inte är klassad

Information som inte är klassad kan t ex avse notislappar, skrivtavlor m m som under kort tid kan infatta information som inte bör nå obehöriga. Det innebär att varje medarbetare vid behov skyddar informationen för onödig/obehörig tillgång.

## Omklassificering

Information kan ibland behöva en annan säkerhetsnivå än de som är klassade ovan. En riskanalys kan till exempel i vissa fall behöva klassas med mycket hög säkerhet. För omklassificering av enskild handling ta kontakt med förvaltningens informationssäkerhetssamordnare (ISSO).

# Märkning av information

Varje enskilt dokument märks inte med sin klassade säkerhetsnivå utan i stället redovisas dokumenttypens säkerhetsnivå. Undantag är genomförda riskanalyser som alltid ska märkas med säkerhetsnivå. Hur säkerhetsklassad information ska hanteras beskrivs i
[*309 Informationssäkerhet*](https://rh.sharepoint.com/sites/Grunddokument/ODMPublished/RH-10863/309%20Informationssakerhet%20RH.docx).

## Märkning av hälso- och sjukvårdsinformation

Den huvudsakliga informationen som hanteras inom vården omfattas av sekretess enligt Offentlighets- och sekretesslagen och den är därför klassad med mycket hög säkerhet. Det finns inget behov av märkning på varje enskilt dokument eftersom patientinformation oavsett media är sekretessbelagd och det är väl känt hos hälso- och sjukvårdspersonal.

|  |
| --- |
| **Relaterade dokument**Rutin Informationsklassning – för informationssäkerhetssamordnare. Informationsklassningsprotokoll |

|  |
| --- |
| **Uppdaterat från föregående version**Ändringar med anledning av byte av ledningssystemsystem.- Justerat rubrik (ej 107)- Justerat taggning (riktlinje i stället för grunddokument) |