3 STYRNING AV INFORMATIONSTILLGÅNGAR

3.1 Mål

All information och övriga informationstillgångar ska vara kopplade till en ägarföreträdare, som har ansvar för att informationen och resurserna klassificeras och skyddas på rätt sätt.

3.2 Utgångspunkt

Informationssäkerhetsarbetet ska ske utifrån generella säkerhetskrav (Säkerhetspolicy och Riktlinjer för informationssäkerhet) och de specifika säkerhetskrav som ställs av verksamheten genom informationsklassificering.

3.3 Märkning av handlingar

Tryckfrihetsförordningen och Offentlighets- och sekretesslagen (2009:400) styr hur allmänna handlingar ska hanteras i offentlig verksamhet. Allmän handling ska lämnas ut på begäran, under förutsättning att den inte omfattas av sekretess.

I Västra Götalandsregionen används följande begrepp, förutom allmän handling, för handlingar:

- Utkast — Minnesanteckning – bakgrundsmaterial som har tillkommit endast för ärendets beredning eller föredragning, dock inte till den del den tillför ärendet sakuppgift.
- Sekretessbelagd — Handling som är sekretessbelagd med stöd av Offentlighets- och sekretesslagen

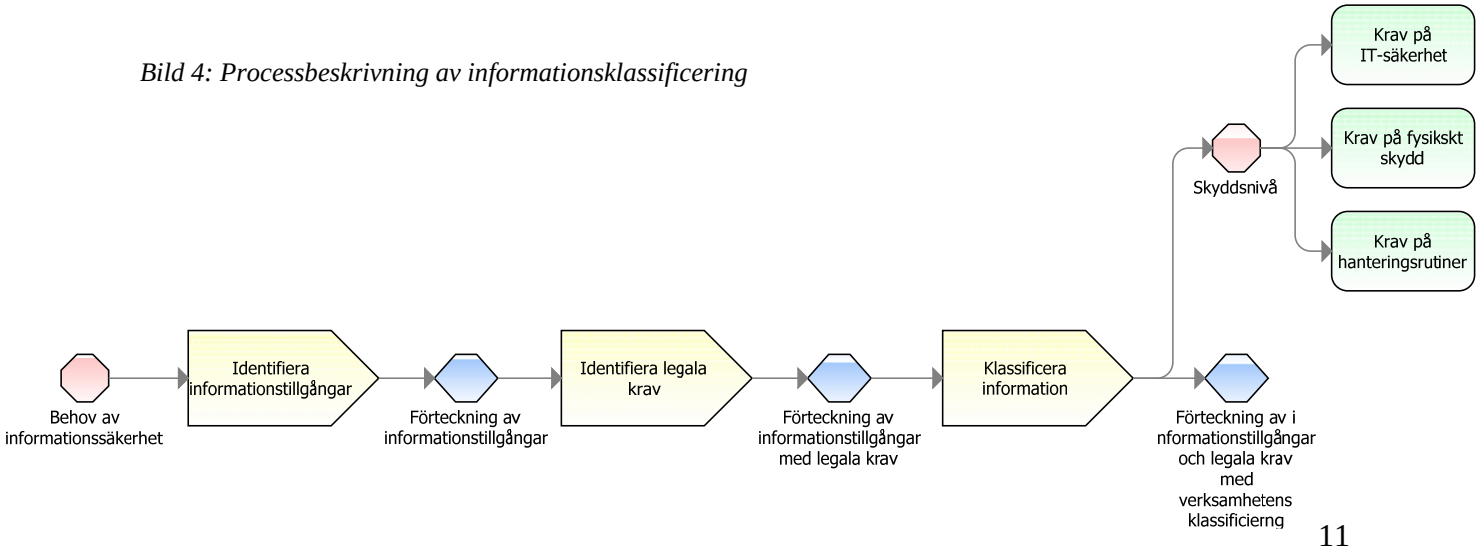
3.4 Informationsklassificering

Informationsägaren ska styra och skydda informationstillgångarna, med utgångspunkt från det värde informationen har för verksamheten. Informationsklassificering är därför en grundläggande aktivitet, för att kravställa skyddsåtgärder och skydda informationen på rätt sätt.

Inom regionens styr- och förvaltningsmodell för IS/IT företräder objektägare verksamhet också informationsägaren och är därmed ansvarig för att informationsklassificering görs ur ett verksamhetsperspektiv och blir en del av objektets dokumentation.

Övriga informationstillgångar, som inte tillhör ett objekt, hanteras inom respektive förvaltning.

Bild 4: Processbeskrivning av informationsklassificering



3.4.1 Identifiera informationstillgångar

Första steget är att identifiera vilken information som hanteras inom avgränsningen för klassificeringen. Utgångspunkten är verksamhetsperspektivet och vilken information som behövs/produceras i verksamhetsprocessen/objektet. Även de resurser som krävs för att hantera informationen identifieras.

3.4.2 Identifiera legala krav

Nästa steg är att identifiera de legala krav som är tillämpliga för hanteringen av informationen och bedöma hur väl de uppfylls. Med legala krav avses lagkrav, föreskrifter och avtal.

3.4.3 Klassificera information

Klassificeringen av informationen bestäms utifrån det värde den har i verksamhetsprocessen och vilka krav på skydd verksamheten ställer utifrån följande begrepp:

- **Tillgänglighet –** möjlighet att utnyttja information efter behov i förväntad utsträckning och inom önskad tid
- **Riktighet** – skydd av information så att den är och förblir korrekt och fullständig
- **Konfidentialitet** – information är tillgänglig endast för den som är behörig att ta del av och använda den
- **Spårbarhet** – möjlighet att i efterhand visa hur och av vem information har hanterats

Klassificeringen genomförs med stöd av VGR:s metod, se *VGR-rutin för klassificering av informationstillgångar*.

Klassificering ska som ett minimum genomföras/aktualiseras vid:

- Etablering av nya IS/IT-system
- Organisations-/processförändringar som kan påverka informationsbehandlingen
- Tekniska förändringar i infrastruktur eller programvaror, som kan påverka informationsbehandlingen
- Om molntjänster eller outsourcing av funktioner eller IS/IT-tjänst övervägs
- Vid allvarliga händelser/incidenter

3.5 Skyddsnivåer

Informationsklassificeringen ska leda till funktionella säkerhetskrav på tekniken samt hanteringsrutiner i verksamheten, som tillsammans uppfyller en säkerhetsnivå som motsvaras av klassificeringen – rätt säkerhet.

3.5.1 Skyddsnivå i verksamhet

Informationsägaren ansvarar för att det finns tydliga rutiner för hur informationen får hanteras i verksamheten.

Reglerna ska omfatta all behandling av information.

Regler och skyddsåtgärder ska omfatta olika typer av bärare av information som USB-minnen, DVD-skivor, ljudinspelningar, fotografier, telefoner, läsplattor, pappersdokument, m.m.

3.5.2 Skyddsnivå IS/IT-tjänster och fysiskt skydd

Resursägaren ansvarar för att det finns tekniska lösningar och administrativa driftrutiner som motsvarar informationsägarens klassificering.
Resursägaren ansvarar för att skyddsåtgärder regelbundet uppdateras och finns med i avtal med extern leverantör av IS/IT-tjänst.

3.6 Säkerhetsdeklaration

För viss typ av IS/IT-tjänst/-funktion är informationsklassificering inte tillämpbart. Då är det lämpligare att genomföra en säkerhetsdeklaration. Syftet med denna är att deklarera vilken säkerhetsnivå tjänsten/funktionen levererar. Detta utgör ett underlag för styrning av användningen. Se *VGR-rutin för säkerhetsdeklaration.*

Resursägaren och informationsägaren ansvarar för att fastställa säkerhetsdeklarationen och, om så behövs, kommunicera hanteringsrutiner.