Riktlinje för systemförvaltning på vård- och omsorgsförvaltningen

Riktlinjen är ett komplement till förvaltningens riktlinjer för informationssäkerhet.

Beslutat av: Omsorgsdirektör
Datum: 2023-12-04
Revideras årligen av: Administrativa avdelningen
Dokumentets giltighet: 2023 - tillsvidare
Dokumentet gäller för: Alla verksamheter
Dokumentansvarig: Administrativa avdelningen

Innehållsförteckning

Inledning

Roller och ansvar kan definieras på många olika sätt. Det viktigaste är att alla ansvarsområden och uppgifter som ingår i systemförvaltning tydligt tilldelas en eller flera personer och att dessa personer får rätt mandat, befogenheter och resurser/tid för att sköta dessa uppgifter.

För verksamhetsspecifika system är det naturligt att en stor del av förvaltningsansvaret ligger hos verksamheten.

För system som används av en annan förvaltning som till exempel Ciceron, Medvind eller Personec är det viktigt att det finns utsedda kontaktpersoner på VOF som agerar **Informationsägare** och **informationsförvaltare** som hanterar de deluppgifter som nämns nedan för systemägare och systemförvaltare

Systemförvaltaren har en del specifika ansvarsområden som alltid måste tillhöra verksamheten. Däröver har också systemförvaltaren en viktig koordinerande roll i hela systemförvaltningsprocessen så nära den verksamheten som är slutanvändare för systemet som möjligt.

Viktiga kunskaper för systemförvaltare är stor kunskap om systemet, kunskap om kravställning och kunskap om informationssäkerhet. Systemförvaltare måste i första hand förstå systemets funktionalitet. För de andra aspekter av systemet behöver systemförvaltaren inte veta allt, men det är viktigt att ha ett bra kontaktnät så systemförvaltare vet vem denne ska fråga om olika aspekter av systemet. Som kontaktperson mot leverantören är det viktigt att systemförvaltare kan ställa krav på systemet. När det gäller informationssäkerhet, är det viktigt för systemförvaltaren att förstå grundprinciperna för informationssäkerhet samt vilken lagstiftning som påverkar systemet.

Det är av vikt att systemförvaltare har en tydlig uppgift att samla all dokumentation rörande systemet (systemförvaltningsplan, SLA, användardokumentation, teknisk dokumentation, incidentrapporter, användarstatistik, …). Detta kräver att IT-driften och/eller leverantören blir ansvariga för att göra denna dokumentation tillgängligt till systemförvaltare och att systemförvaltare blir ansvariga för att se till att dokumentationen samlas in och sedan görs tillgängligt för alla intressenter.

Det är viktigt att skilja på rollerna systemägare och systemförvaltare och det får inte vara samma person.

Ansvar och uppföljning

- Tillämpning och uppföljning av Riktlinje systemförvaltning VOF tillfaller chefer på alla nivåer.

Systemägare

Den som har det övergripande ansvaret för systemet[1] och dess nyttjande i verksamheten. Systemägaren beställer, prioriterar och godkänner förändringar i systemet, samt följer upp systemets prestanda, kvalitet och kostnad.

Utses av förvaltningschef. I de fall ett IT-stöd saknar systemägare tar förvaltningschef denna roll tills annan person utses. Systemägaren kan vid behov också utse en biträdande systemägare som stöttar den ordinarie systemägaren i sitt ansvar. Biträdande systemägare agerar då i systemägarens ställe, med rapporteringsansvar till systemägaren. Viktigt är att varken systemägare eller biträdande systemägare får ha fler roller inom systemförvaltningsorganisationen.

Systemägarens ansvar

- har budgetansvar för systemet och godkänner beställningar av ändringar och uppdateringar.
- är formellt ansvarig för att funktionaliteten och kvaliteten av systemet motsvarar verksamhetens behov, detta innebär också formellt ansvar för systemets informationssäkerhet.
- tar det formella beslutet om behörigheter inom systemet.
- utser lämplig systemförvaltare och ger systemförvaltaren de resurser och befogenheter som behövs.
- Ansvarar för avtal med leverantör
- Godkänner säkerhetsklassificering och riskanalys
- Godkänner systemförvaltningsplan

Systemförvaltare

Den som leder och samordnar systemförvaltningsarbetet, samt fungerar som en länk mellan systemägare, systemleverantör och systemanvändare. Systemförvaltaren planerar, genomför och dokumenterar förändringar i systemet, samt ansvarar för systemets drift, underhåll och support.

Systemförvaltarens ansvar

- skriver en årlig systemförvaltningsplan som beskriver systemförvaltningens utgångsläge, mål, planerade aktiviteter, resursbehov och organisation.
- följer kontinuerligt upp att systemförvaltning sker enligt planen (både tidsmässigt och kvalitetsmässigt).
- koordinerar utbildning av användare och uppdaterar användardokumentation.
- koordinerar kommunikation mellan IT/leverantör och verksamheten och samlar in synpunkter från användare som underlag till prioritering av ändringar.
- initierar ändringshanteringen, agerar beställare mot IT-enheten, följer upp och godkänner ändringar innan de driftsätts.
- rapporterar regelbundet till systemägare om systemförvaltningen för systemet.
- bevakar aktivt incidenthanteringen för systemet, följer upp större incidenter och samlar statistik om alla driftärenden som rör systemet.
- koordinerar arbetet med informationssäkerhet för systemet, ser till att riskanalyser genomförs och avbrottsplaner skrivs och klassificering av information görs och att denna information hålls uppdaterad.
- samlar in systemdokumentation (användardokumentation, teknisk dokumentation, driftdokumentation, mm).
- informerar alla intressenter om viktiga händelser i systemet.

[1] *Informationssystem, IT-system, Robotar, E-tjänster, Molntjänster etc.

- är första kontaktperson om systemet mot leverantören, mot IT-enheten och mot användare.

Informationsägare

En informationsägare är en roll som innebär ett utpekat ansvar för information inom ett eller flera verksamhetsområden och hanteras inom den egna verksamheten.
Utses av förvaltningschef.
En informationsägare kan vara en person, en funktion eller en grupp av personer som har befogenhet att fatta beslut om informationen. En informationsägare kan också delegera vissa uppgifter till andra roller, till exempel systemägare, systemförvaltare eller systemleverantör. En informationsägare ska dock alltid ha det yttersta ansvaret för informationen och dess säkerhet.

Informationsägaren är den som ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids. Informationsägaren är därmed riskägare för den information som ska hanteras i IT-systemet. För att hantera risken bör informationsägaren genomföra en riskanalys. Om det finns flera informationsägare som ska använda IT-systemet bör samtliga delta i riskanalysen.

Eftersom skadeverkningarna av bristande säkerhet i IT-systemet uppstår hos informationsägaren är det informationsägaren som måste bedöma risker och ställa krav bland annat genom informationsklassning.

De interna relationerna mellan informationsägare och systemägare bör, när det gäller informationssäkerhet, utgå från informationsägaren. Kan vara en förvaltningschef/verksamhetschef.¨

Informationsägarens ansvar

- Definierar verksamhetens informationsbehov
- Kravställare för informationssäkerhet
- Ansvarar för informationssäkerhetsklassning
- Kravställare för informationskvalitet
- Kravställare för behörighet till information
- Ansvarar för att informationen följer lagar, förordningar och interna styrdokument
- Hantera incidenter och risker som rör informationen.
- Informera och utbilda användare om informationssäkerhet.
- Kravställare för backup

Systemanvändare

Den som använder systemet i sitt dagliga arbete, samt ger feedback och förslag på förbättringar i systemet. Systemanvändaren ansvarar för att följa de regler och rutiner som gäller för systemet, samt rapportera eventuella fel eller problem i systemet till systemförvaltaren eller systemleverantören**.**

Systemleverantör

Den som levererar systemet och dess komponenter, samt utför förändringar i systemet enligt systemägarens och systemförvaltarens krav och önskemål. Systemleverantören ansvarar för systemets tekniska kvalitet, funktionalitet och säkerhet.

Förvaltning av verksamhetskritiska IT-stöd eller IT-stöd med känslig information

Ett IT-stöd som är av karaktären verksamhetskritiskt eller där det sker behandling av känslig information (t.ex. sekretess enligt Offentlighets- och sekretesslagen) ska basera sin systemförvaltning på ett systematiskt informationssäkerhetsarbete.

Detta innebär att:

- En informationssäkerhetsklassning av IT-stödet/objektet ska finnas
- En riskanalys ska årligen och vid förändring genomföras av IT-stödet/objektet utifrån klassningen
- De åtgärder som tas fram i riskanalysen ska utgöra grund för aktiviteter i kommande års systemförvaltningsplan

Säkerhetsstrateg

Säkerhetsstrategen ska leda, utveckla, samordna och följa upp informationssäkerhetsarbetet utifrån förvaltningens styrande dokument. Utöver det ska säkerhetsstrategen:

- Informera, utbilda och ge råd
- Samarbeta med förvaltningens dataskyddsombud med att stödja verksamheten vid genomförandet av informationsklassificering och olika typer av riskbedömningar inkluderande konsekvensanalyser avseende dataskydd enligt dataskyddsförordningen
- Informera Omsorgsdirektören/informationsägaren om legala krav inte efterlevs.
- Delta i framtagande av förvaltningsövergripande styrande dokument avseende informationssäkerhet.
- Samarbeta med övriga säkerhetsområden med målet att säkerhetsåtgärder blir välbalanserade och heltäckande samt samråda med övrig kompetens inom förvaltningens kansli
- Delta vid informationssäkerhetsincidenter inom förvaltningen.
- Samråda med dataskyddsombud kring hantering av personuppgiftsincidenter och dataintrångsärenden inom förvaltningen

Förvaltningsmöten

För alla IT-system bör det hållas ett eller flera systemförvaltningsmöten per år. För stora, komplexa och kritiska IT-system kan det vara befogat med månadsmöten.

Nedan följer exempel på agenda för förvaltningsmöten. Detta måste förstås anpassas utifrån berört IT-system.

1. Incidenter och problem
    a. Nya, allvarliga, incidenter (sedan förra mötet)
    b. Status åtgärdslogg över incidenter och bakomliggande problem
2. Förvaltnings-och utvecklingsaktiviteter
    a. Status planerade aktiviteter (förvaltning och utveckling)
    b. Förslag på nya aktiviteter, nya inkomna ärenden
    c. Status återkommande aktiviteter
    d. Systemförvaltningsplan
        i. Översyn och borttag av behörigheter
        ii. Översyn av riskregister
        iii. Översyn av informationssäkerhetsklassning
3. Ekonomi, avtal m.m.
    a. Ekonomiskt utfall jämfört med budget, ev. timbankar, m.m.
    b. Licensutnyttjande
    c. Avtalsfrågor