Gäller för: Fastighet stöd och service
Innehållsansvar: Annika Sonesson, (annso80), Enhetschef
Granskad av: Flera granskare finns - se eftersättsblad
Godkänd av: Måns Ottertun, (manot1), Kanslichef
Giltig från: 2024-10-25
Giltig till: 2029-09-30

Rutin avseende ansvar för IS/IT-system

Rutin avseende roller och ansvar för förvaltningens IS/IT-system. Rutinen täcker in behörighetsstyrning, med hänseende till livscykelhantering av behörigheter i förvaltningens IS/IT-system, som inkluderar tilldelning, kontroll samt avslut av behörigheter. Rutinen baseras på regionala rutiner inom Ledningssystem för informationssäkerhet och dataskydd (LISD). Regional riktlinje informationssäkerhet och dataskydd

Förändringar sedan föregående version

Ny rutin

Syfte

Det ska vara tydligt i förvaltningen vem som ansvarar för vad för förvaltningens IS/IT-system. Användare av IS/IT-system ska ha tillgång till rätt information på rätt sätt för sin arbetsuppgift och vara medveten om sitt personliga ansvar. Målet är att uppnå applikationssäkerhet i syfte att skydda informationens riktighet, integritet och tillgänglighet. Att åtkomst till IS/IT-system och dess information ska ges enligt klart definierade principer, tydliga ansvarsförhållanden och enhetliga metoder. Behörigheter ska utfärdas genom att göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken närmare information olika personalkategorier och olika slags verksamheter behöver.

Ansvar

Informationsägarskapet sammanfaller med ansvaret i verksamheten, till exempel ansvarar en avdelningschef för information inom avdelningen, eller en processägare för informationen inom processen. När informationstillgångarna ingår i regiongemensamma verksamhetsprocesser, IS/IT-

tjänster/system, projekt och/eller upphandlingar företräds flera myndigheters informationsägare av en regional processägare. När informationstillgångarna ingår i verksamhetssystem så fördelas ansvaret mellan systemägare och linjechef. Det operativa arbetet med livscykelhanteringen av behörigheter är ofta vidare fördelat till personal såsom systemförvaltare eller liknande.

Roller med ansvar

Systemägare ansvarar för att;

- Sätta den långsiktiga strategin för systemet och att budget för systemet är säkerställt.
- Verkställa de beslut kring systemet som tas av verksamhetsledningen.
- Säkerställa att systemet är informationsklassat och riskbedömt
- Säkerställa att det finns en systemförvaltningsorganisation.
- Säkerställa att det finns användarstöd (support, utbildning och lathundar) för systemet.
- Besluta om nyutveckling, vidareutveckling och avveckling av systemet.
- Tillse att det finns manuella rutiner vid avbrott.

Systemägaren är informationsägare för den information som hanteras i systemet och beslutar om vilka säkerhetsåtgärder som krävs för åtkomst till informationstillgångar baserat på genomförd informationsklassning och riskbedömning.

Systemägaren är behörighetsägare för systemet och ansvarar för att det finns en, utifrån informationens värde, lämplig behörighetsmodell genom att;

- Säkerställa att behörighetstilldelningen är ändamålsenlig och uppfyller de krav som ställs enligt dataskyddsförordningen, patientdatalagen och Socialstyrelsens föreskrifter.
- Verkställer att behörighetsmodellen efterlevs genom att ansvara för att rätt personer har tillgång till rätt information och funktion i systemstödet.
- Beslutar om förändringar i behörighetsmodellen.
- Godkänner avsteg från behörighetsmodellen.
- Ansvarar för att årlig behörighetsrevision utförs.

Systemägare ska utses genom ett beslut i en verksamhetsledning. Det ska bara finnas en systemägare för ett system. Systemägaren

ska ha en övergripande kunskap om aktuellt systemstöd samt verksamheten som IT-systemet stödjer.

Systemförvaltare ansvarar för att;

- Det finns en livscykelplanering av systemet, så som plan för införande av nya versioner.
- Ha kontakt med leverantör (inklusive leveransorganisationens hos Koncernstab Digitalisering) för systemet.
- Bevaka att det finns ett giltigt avtal för systemet.
- Tillse att beslutade systemanpassningar utförs både när det gäller nyutveckling, vidareutveckling samt avveckling av systemet.
- Stödja systemets användarstöd (support, utbildning och lathundar).
- Tillse att de säkerhetsåtgärder som krävs för åtkomst till informationstillgångar baserat på genomförd informationsklassning och riskbedömning genomförs.
- Tillse att behörighetsmodellen i systemet realiseras enligt beslut.
- Tillse förändringar i behörighetmodellen.
- Ta fram underlag från systemet inför årlig behörighetsrevision.
- Tillse att förändringar utifrån årlig behörighetsrevision genomförs.
- Ha ett informationsansvar (informera om nya versioner, pågående incidenter osv) till berörd verksamhet/ användare av systemet.

Systemförvaltaren utses av systemägaren. Det ska bara finnas en systemförvaltare för ett system. Systemförvaltaren ska ha god kunskap om aktuellt systemstöd samt verksamheten som IT-systemet stödjer.

Samordningsansvarig IS/IT (SIS)

Samordningsansvarig IS/IT är en regional roll.

Uppdragsbeskrivning för Samordningsansvarig IS/IT

För Fastighet, stöd och service finns följande verkställighetsbeslut för bemanning av rollen som Samordningsansvarig IS/IT.

Verkställighetsbeslut gällande samordningsansvar IS/IT

Linjechef/ansvarig chef/uppdragsgivare ansvarar för att;

- Medarbetare/konsult har åtkomst till rätt verksamhetssystem med rätt behörighetsnivå
- Säkerställa att medarbetare får den utbildning som krävs för att arbeta i de verksamhetssystem som behövs för att utföra sina arbetsuppgifter
- Informera medarbetare/konsult om gällande regelverk kopplat till användning av IS/IT-system och utrustning
- Förmedla förändringar av anställning/roll för att korrigera alternativt avsluta behörigheter.
- Beställa och avsluta särskilda-/priviligierade rättigheter (SA- och KA-konto)
- Beställa och avsluta VPN

Medarbetare/konsult ansvarar för att;

- Ha kunskap i de verksamhetssystem som behövs för att utföra sina arbetsuppgifter
- Ha förståelse för värdet av informationen och varför den ska skyddas samt ha tillräcklig kompetens för att kunna utföra sina arbetsuppgifter på ett säkert sätt.
- Följa Västra Götalandsregionens regler för datoranvändning och andra regelverk kopplat till IT och informationssäkerhet
- Ansvarar själv under sin anställningstid för en säker hantering av sina inloggningsuppgifter. Inte avslöja eller låna ut sina personliga login.

Omfattning

Rutinen omfattar behörigheter som tilldelas för:

- Verksamhetssystem
- Särskilda-/priviligierade rättigheter (SA- och KA-konto)

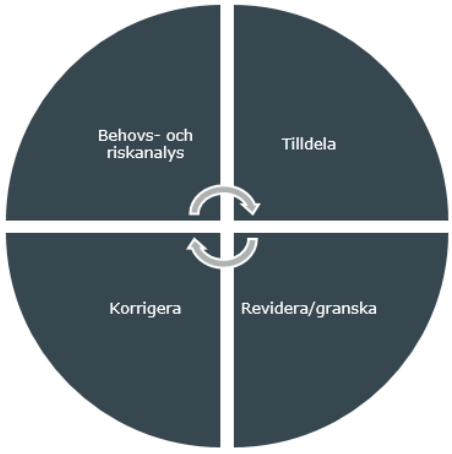
- KA-konto (Klient Admin) är ett personligt konto och är den kontotyp som används för att få behörigheten lokal administratör på klienter, där ett vanligt användarkonto inte är tillräckligt.
- SA-konto ger server access
- Priviligierade åtkomsträttigheter ska tilldelas restriktivt och ställer högre krav på exempelvis loggning och uppföljning.

Utförande

Behörigheter ska livscykel hanteras samt baseras på medarbetarens arbetsuppgifter och organisatorisk tillhörighet. Varje användares digitala identitet ska kunna verifieras och alltid vara spårbar till en fysisk person.

Villkor och rutiner för vilka som får behörighet ska föregås av en behovs- och riskanalys för att säkerställa rätt behörighet och vilka risker det kan innebära om personen har för lite eller för mycket tillgång till olika uppgifter. För att kunna säkerställa korrekt användning av behörigheter behöver i vissa fall loggning och uppföljning genomföras.

Nedan beskrivs de aktiviteter som ingår i livscykelhanteringen av behörigheter samt utförandet av dessa.



Bilden beskriver livscykelhanteringens olika faser som bygger på PDCA

Aktivitet	HUR	Ansvarig	Utförare kan vara
Behovs- och riskanalys	Behov bedöms utifrån vad en medarbetare behöver för att utföra sina dagliga arbetsuppgifter.	Process-/Systemägare	Linjechef Systemförvaltare Processledare SIS (gäller främst SA- och KA-konto)

	Saknas informationsklassning ska den utföras för att matcha den med behörighetsmodellen. Risker bedöms utifrån informations-klassningen och informationens betydelse för verksamheten. Identifiera och analysera risker för enskildas personliga integritet eller annan skyddsvärd information. Värdering ska också göras kring behovet av utbildning innan behörighet tilldelas. Utbildning omfattar regelverk som styr informations-hanteringen, dataskydd och applikations-utbildning. Lämpligt är att behörigheter är individuella med definierade åtkomstprofiler för olika roller/befattningar, till exempel administratör, beställare, utförare, uppföljning etcetera För särskilda/ priviligierade behörigheter gäller samma princip med behovs- och riskanalys.		Konsulteras vid informationsklassning och riskhantering: Informationssäkerhetsansvarig
Tilldela	Behörighetsnivån styrs av behovet kopplat till risk av tillgång till information och informations-behandlingsresurser. Tilldelning utförs om behoven stämmer överens med framtagna kriterier för åtkomst. Verksamhetssystem Om ansökan betraktas som avvikande, dvs behoven matchar inte kriterierna, ska process-/systemägare göra en bedömning och ge tillstånd om aktivering av behörigheten. Särskilda/ priviligierade behörigheter (SA/KA) Om ansökan betraktas som avvikande, dvs behoven matchar inte kriterierna, ska IS/IT chefen ge tillstånd om aktivering av behörigheten.	Process-/Systemägare/IS/IT-chef	Systemförvaltare – gällande verksamhetssystem SIS - gällande särskilda-/priviligierade rättigheter (SA- och KA-konton)
Revidera/granska	Behörighetsmodell och behörigheter ska årligen granskas och revideras för att säkerställa att dessa är riktiga och aktuella. Förändring av anställning, ny/borttagen roll och avslutad	Process-/Systemägare/IS/IT chef	Systemförvaltare • Revidera behörighetsmodellens tillförlitlighet i förhållande till informationsklassningen

	anställning inom VGR kan föranleda en korrigering eller borttagning av medarbetares åtkomsträttigheter. Samtidigt uppdateras behovs- och riskanalysen.		• Ta fram utdrag över aktiva behörigheter i verksamhetssystem SIS funktion (förvaltning digital arbetsplats) • Utdrag över aktiva särskilda-/priviligierade rättigheter (SA- och KA-konton) Linjechef/ansvarig chef/uppdragsgivare • Granska och ge förslag till revidering • Att ha en förteckning över medarbetares åtkomst till olika system
Korrigera	Korrigering/borttag ska alltid utföras under kontrollerade former, utan dröjsmål, och föregås av en behovs och riskanalys.	Process-/Systemägare	Systemförvaltare • Utför korrigering/borttag efter samma princip som vid tilldelning SIS • Utför korrigering/borttag efter samma princip som vid tilldelning

Relaterade dokument

Regional riktlinje informationssäkerhet och dataskydd

Information om handlingen

Handlingstyp: Rutin

Gäller för: Fastighet stöd och service

Innehållsansvar: Annika Sonesson, (annso80), Enhetschef

Granskad av: Ior Berglund, (iobe1), Direktör, Erik Hallberg, (eriha1), Regionområdeschef, Gabriella Köhler Graf, (gabgr3), Regionområdeschef, Thomas Bjarnemo, (thobj2), Regionområdeschef, Eva Orban Degerman, (evade7), Regionområdeschef, Britt Olsson, (briol3), Ekonomichef, Marianne Päämaa, (marpa85), HR-chef, Hanna Freij, (hanfr32), Kommunikationschef

Godkänd av: Måns Ottertun, (manot1), Kanslichef

Dokument-ID: SFSS12798-2040028314-7

Version: 1.0

Giltig från: 2024-10-25

Giltig till: 2029-09-30