Gäller för: Västra Götalandsregionen
Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare
Godkänd av: Johan Flarup, (johfl), Direktör
Giltig från: 2024-08-05
Giltig till: 2026-07-28

Regional rutin för IT-säkerhetsspecifikation

Ledningssystem för informationssäkerhet

Rubrik: IT-säkerhetsspecifikation - Regional rutin 2024 - 2028
Dokument-ID: RS10162-1596316381-111
Version: 3.0

VÄSTRA GÖTALANDSREGIONEN

Innehåll

Sammanfattning

Mål: Verksamheten ska identifiera vilken information och andra relaterade informationstillgångar som finns och fastställa dess betydelse för verksamheten. Informationsbehandlingsresurser ska klassas och skyddas på rätt sätt.

Informationssäkerhetsarbetet ska ske utifrån organisationens säkerhetskrav och de specifika krav som ställs av verksamheten genom informationsklassning. Samtliga informationstillgångar, inklusive informationsbehandlingsresurser, ska skyddas utifrån det behov av skydd som identifierats.

En IT-säkerhetsspecifikation syftar till att tydliggöra vilken nivå av säkerhet en IS/IT-tjänst har och tydliggör de säkerhetsåtgärder som är implementerade, vilket sedan utgör ett underlag för styrning. Det förutsätter ett systematiskt och riskbaserat informationssäkerhetsarbete vid utformning och inför driftsättning av IS/IT-tjänster.

För informationsägaren skapar IT-säkerhetsspecifikationen en förståelse för vilka informationstillgångar som är tillåtna att hanteras i IS/IT-tjänsten och därmed också vilka kompletterande säkerhetsåtgärder som verksamheten behöver vidta utifrån informationsklassningens krav.

Denna rutin är styrande för alla förvaltningar och bolag i Västra Götalandsregionen och ingår i ledningssystemet för informationssäkerhet och dataskydd (LISD).

1. Ansvar

Ansvar för informationssäkerhetsarbetet följer linjeansvaret. Koncernstab digitalisering ansvarar för utveckling, drift och förvaltning av regiongemensamma IS/IT-tjänster. Alla IS-IT-tjänster ska ha en utpekad ägare som ansvarar för att införa, förvalta och utvärdera lämpliga säkerhetsåtgärder så att adekvat skydd uppnås i IS/IT-tjänsten. Säkerhetsåtgärderna ska ge ett tillräckligt skydd och motsvarar informationsägarens eller dess företrädares krav på skyddsbehov, vilket förutsätter god insyn i informationsägarens verksamhet.

1.1 Ägare av IS/IT-tjänst

Ägare av IS/IT-tjänst har ansvar för att, utifrån de krav som ställs på tjänsten genom informationsklassningen och utifrån de risker som identifierats, att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder i IS/IT-tjänsten så att adekvat skydd uppnås i tjänsten.

Vidare ansvarar ägare av IS/IT-tjänst för att bedriva ett systematiskt informationssäkerhetsarbete, vilket innebär att arbeta förebyggande och att kontinuerligt anpassa skyddet utifrån verksamhetens behov och de riskbedömningar som genomförts.

Det operativa arbetet med att genomföra en IT-säkerhetsspecifikation kan vara delegerat.

Ägare av IS/IT-tjänst ansvarar för att IT-säkerhetsspecifikationen upprättas som en allmän handling i diariet och därefter kontinuerligt utvärderas och uppdateras.

I projekt

Om ett projekt syftar till implementation av ny IS/IT-tjänst är det projektet som ska säkerställa att en IT-säkerhetsspecifikation upprättas. IT-säkerhetsspecifikationen blir en del av den dokumentation som sedan överlämnas till ägare av IS/IT-tjänst.

2. När ska en IT-säkerhetsspecifikation göras?

IT-säkerhetsspecifikation för IS/IT-tjänst ska tas fram eller justeras före tjänst eller förändringar i tjänst tas i drift eller om en IT-säkerhetsspecifikation inte tidigare tagits fram.

Förändringar i interna och legala krav, infrastruktur och/eller leverans som kan påverka eller förändra implementationen av säkerhetsåtgärder ska bevakas och hanteras av ägare av IS/IT-tjänsten.

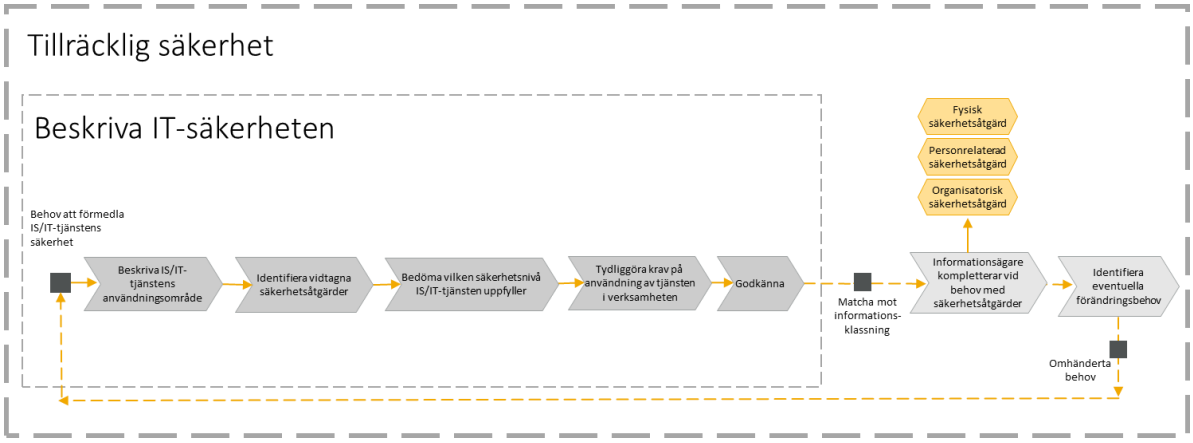
3. Genomförande

Att beskriva IT-säkerheten hos en IS/IT-tjänst är en process som syftar till att tydliggöra tjänstens säkerhet, vilket ska bidra till att skapa förståelse för vilka säkerhetsåtgärder tjänsten har och vilka säkerhetsåtgärder informationsägaren behöver komplettera med för att uppfylla en säkerhetsnivå som motsvaras av informationsklassningen – tillräcklig säkerhet. Säkerhetsåtgärder ska vara ändamålsenliga och proportionerliga och utgå från informationens skyddsvärde. Vid beslut om lämplighet ska därför faktorer som informationens skyddsbehov, risk och kostnadseffektivitet beaktas. För att nå tillräcklig säkerhet är det av vikt att det finns ett samspel mellan ägare av IS/IT-tjänsten och informationsägaren eller dess företrädare.

Säkerhetsåtgärder är åtgärder för att bibehålla och/eller förändra risk och delas upp under fyra teman:

- Tekniska säkerhetsåtgärder
- Fysiska säkerhetsåtgärder
- Personrelaterade säkerhetsåtgärder
- Organisatoriska säkerhetsåtgärder

IT-säkerhetsspecifikationen innehåller en sammanfattning av implementerade säkerhetsåtgärder för en given IS/IT-tjänst.



Figur 1 Processen för IT-säkerhetsspecifikation i förhållande till en säkerhetsnivå som motsvaras av informationsklassningens behov – tillräcklig säkerhet.

3.1 Beskriva användningsområde

För att kunna upprätta en IT-säkerhetsspecifikation behöves kunskap om hur IS/IT-tjänsten är tänkt att användas i verksamheten, dess syfte, vem eller vilka som är informationsägare och vilka beroenden som finns till andra interna och externa tjänster. Börja därmed att skapa en översiktlig bild av IS/IT-tjänstens funktionalitet och användningsområde.

Framtagande av IT-säkerhetsspecifikation förutsätter att det bedrivs ett systematiskt och riskbaserat informationssäkerhetsarbete.

Utgå från verksamhetens informationsklassning vid identifiering av vilken information som anses lämplig att behandla i tjänsten.

3.2 Identifiera säkerhetsåtgärder

Beskriv vilka säkerhetsåtgärder som är implementerade i IS/IT-tjänsten. Om tjänsten behandlar personuppgifter behöver det även framgå vilka säkerhetsåtgärder som implementerats som säkerställer lämpligt skydd för personuppgifter.

Hjälp i arbetet kan vid behov lämnas av regionala stödfunktioner inom informationssäkerhet och cybersäkerhet. Det är också lämpligt att begära in relevanta underlag från leverantör.

3.3 Bedöma säkerhetsnivå

Utgångspunkten är att IS/IT-tjänsten så långt det är möjligt, lägst ska ha en säkerhetsnivå och de säkerhetsåtgärder som motsvarar informationsklassningens behov.

Utifrån *Vägledning säkerhetsåtgärder*, bedöm vilken informationsklass tjänsten uppfyller kraven för.

Utifrån *Vägledning legala krav,* bedöm vilka lagrum tjänsten uppfyller kraven för.

3.4 Tydliggöra krav på användning

Tydliggör om det finns särskilda krav på verksamheten som gäller innan och/eller vid användning av IS/IT-tjänsten – eller om det finns begränsningar i tjänsten som medför att viss information inte är tillåten att hantera.

3.5 Godkänna

IT-säkerhetsspecifikationen dokumenteras i regional mall som finns publicerad på intranätet. Den granskas av ägare IS/IT-tjänst. Ett digitalt gransknings- och godkännandeflöde i diariesystemet är tillräckligt.

IT-säkerhetsspecifikationen är en allmän handling och hanteras i enlighet med myndighetens informationshanteringsplan. Ägaren av IS/IT-tjänsten eller den som företräder densamma har ansvar för att kommunicera IT-säkerhetsspecifikationens innehåll till berörda i organisationen, vilket innebär kommunikation till både verksamhetsrepresentanter, informationsägare eller dess företrädare.

4. Komplettera med övriga säkerhetsåtgärder

Informationssäkerhet uppnås genom att en lämplig uppsättning säkerhetsåtgärder införs, och ofta behöver exempelvis tekniska säkerhetsåtgärder kombineras med både organisatoriska, fysiska och personrelaterade. För att nå en tillräcklig nivå av säkerhet krävs ett samspel mellan ägare av IS/IT-tjänst och verksamhet.

Vad olika säkerhetsåtgärder innebär går att läsa mer om under relaterade dokument svensk standard SS-ISO/IEC 27002:2022.

5. Identifiera förändringsbehov

Förändringsbehov som identifieras bör vara en del av den samlade systemdokumentationen för IS/IT-tjänsten. Om det finns behov från

informationsägaren om ett utökat skydd, behöver IS/IT-tjänstens säkerhetsåtgärder motsvara det ökade skyddsbehovet.

Relaterade dokument

Följande dokument är relaterade till rutin för IT-säkerhetsspecifikation:

- Riktlinje för informationssäkerhet och dataskydd
- Säkerhetsåtgärder i svensk standard SS-ISO/IEC 27002:2022
- Vägledning Säkerhetsåtgärder
- Vägledning legala krav

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-111

Version: 3.0

Giltig från: 2024-08-05

Giltig till: 2026-07-28