STYRANDE PRINCIPER FÖR DIGITAL SAMVERKAN

Sammanfattning

De styrande principerna för digital samverkan utgör en säker grund för digital samverkan mellan kommuner, landsting, stat, privata utförare och invånare för att bygga den tillit som behövs för att möjliggöra säkert digitalt informationsutbyte.

De styrande principerna för digital samverkan säkerställer att alla aktörer agerar på ett likartat, jämförbart och kostnadseffektivt sätt. Principerna leder också till en bredare och smartare användning av redan gjorda investeringar och principerna minskar risken för felinvesteringar och särlösningar.

Informationssäkerhet:

1. *att* ha en antagen informationssäkerhetspolicy med tillhörande riktlinjer
2. *att* ha en utsedd person som leder och samordnar informationssäkerhetsarbetet
3. *att* tillämpa en likvärdig metod och jämförbara nivåer för informationsklassificering
4. *att* tillse att resultatet av informationsklassificeringen leder till reella skyddsåtgärder
5. *att* utifrån återkommande riskanalyser och inträffade incidenter vidta nödvändiga åtgärder för att upprätthålla rätt skyddsnivåer

Tillit:

6. *att* tillämpa gemensamma tillitsramverk för att skapa tillit över huvudmannagränser
7. *att* koppla informationstillgångar till relevanta tillitsnivåer

Federering:

8. *att* ha förmågan att utfärda och/eller konsumera elektroniska identitets- och behörighetsintyg
9. *att* säkerställa att alla delar i det elektroniska identitets- och behörighetsintyget följer aktuella tillitsramverk
10. *att* kravställa federativ förmåga i varje tjänst

Bakgrund

Informationssäkerhetsarbetet i kommunerna i Gävleborgs län bedrivs med skiftande kvalité. En kraftsamling behöver ske, dels för att bättre upprätthålla informationssäkerheten inom varje organisation och dess informationstillgångar, dels för att möjliggöra digital samverkan med medborgare och mellan kommuner, landsting, stat och privata utförare utan att äventyra informationssäkerheten för varje berörd informationstillgång.

Behovet av att förtydliga, strukturera och effektivisera informationssäkerhetsarbetet har påtalades av revisorerna i flera kommuner vilket också tydligt synliggör gapet för uppfyllnad av de regulatoriska kraven såsom personuppgiftslagen (1998:204), lagen om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (2006:544) , Patientdatalagen (2008:355) och Socialstyrelsens föreskrifter (2008:14). Det innebär dessutom stora risker för kommunen ekonomiskt, verksamhetsmässigt och inte minst, för medborgarnas förtroende.

Länets kommuner har inspirerats av *de 16 principer för samverkan* som arbetats fram av Kommunförbundet i Stockholm mot bakgrund av samma utmaning som kommunerna i länet har och som visat sig haft positiva effekter på så väl informationssäkerhetsarbetet som samverkan i digital samverkan med medborgare och över huvudmannagränser.

Länets kommuner väljer att i huvudsak fokusera på de principer som tar fasta på att upprätthålla informationssäkerheten samt har valt att komplettera med ytterligare en princip för att säkerställa en reell tillämpning av informationssäkerhetsarbetet.

För att underlätta ett införande av de styrande principerna för samverkan har representanter från i princip samtliga kommuner och landstinget inom regionen tillsammans arbetat fram färdiga förslag till informationssäkerhetspolicy, riktlinjer för informationssäkerhet, , användarinstruktioner, instruktioner för informationsklassificering och riskanalys. Vidare finns en överenskommelse om att gemensamt utarbeta, tillämpa och förvalta en förenklad säkerhetsarkitektur.

Målsättningen är att länets samtliga kommuner, landsting och de organisationer som kommer i kontakt med berörda informationstillgångar antar principerna.

Princip #1 - *att* ha en antagen informationssäkerhetspolicy med tillhörande riktlinjer

Syfte & nytta

En informationssäkerhetspolicy är ett övergripande dokument som anger mål och inriktning samt ger styrning och uppföljning av informationssäkerhetsarbetet.

Grundelementet i arbetet med informationssäkerhet är ledning och styrning. För att en organisations ledning ska kunna styra informationssäkerhetsarbetet så att det motsvarar de behov som organisationen har, krävs ett ledningssystem för informationssäkerhet (LIS). Ledningssystemet omfattar bland annat policy, styrdokument, olika modeller för exempelvis riskanalys och uppföljning. Syftet med LIS är också att skapa den säkerhetskultur som gör alla medarbetare aktiva i säkerhetsarbetet.

Utmaning

Etablering av ett ledningssystem för informationssäkerhet (LIS) är resurskrävande och det kräver ledningens engagemang.

Mål

För att uppnå målet med denna princip ska den egna organisationen implementerat en informationssäkerhetspolicy med tillhörande riktlinjer.

Princip #2 - *att* ha en utsedd person som leder och samordnar informationssäkerhetsarbetet

Syfte & nytta

Informationssäkerhet handlar många gånger mer om samordning än ledning. En eller flera utsedda personer som kan ge kvalificerad strategisk- och operativ rådgivning till ledning och verksamhet ur ett brett informationssäkerhetsperspektiv är en tillgång för organisationen. Det är naturligt att den eller de som är utsedda också utvecklar och upprätthåller regelverk, policys och riktlinjer samt initierar, utför och följer upp revisioner och kontroller.

Utmaning

Små och medelstora organisationer har sällan möjlighet att ha tilldelade resurser som leder och samordnar informationssäkerhetsarbetet utan arbetsuppgiften delas sannolikt med andra arbetsuppgifter. Organisationer som inte har något konkurrensförhållande, exempelvis kommuner, har visat prov på att denna typ av funktion kan delas organisationer i mellan.

Mål

För att uppnå målet med denna princip ska organisationen ha minst en utsedd person som leder och samordnar informationssäkerhetsarbetet

Princip #3 - *att* tillämpa en likvärdig metod och jämförbara nivåer för informationsklassificering

Syfte & nytta

Syftet med informationsklassificering är att ge en informationstillgång en lämplig skyddsnivå i förhållande till informationstillgångens värde och de hot som omger den.

En informationsklassad informationstillgång ger bästa tänkbara grund för att bestämma lämpliga skyddsåtgärder för informationstillgången.

Utmaning

Informationsklassificering är i ett inledande skede resurskrävande. Resultatet av en informationsklassificering kräver att den som har i uppgift att skydda informationen, exempelvis en IT-avdelning eller en driftpartern, har förmågan att anpassa sig till resultatet och att organisationen tydligt uttalat konsekvenserna av en klassning.

Mål

För att uppnå målet med denna princip ska den egna organisationen klassificera sina informationstillgångar med utgångspunkt i säkerhetsaspekterna konfidentialitet (tidigare benämnt sekretess), riktighet, tillgänglighet och spårbarhet.

Klassificeringen bör genomföras likvärdigt eller jämförbart med Myndigheten för samhällsskydd och beredskaps (MSB) och Swedish Standards Institute (SIS) metod för informationsklassning.

Princip #4 - *att* tillse att resultatet av informationsklassificeringen leder till reella skyddsåtgärder

Syfte & nytta

Syftet är att varje informationstillgång ska få lämpliga skydd i förhållande informationstillgångens värde och de hot som omger den.

Utmaning

Utmaningen är att omsätta resultatet av informationsklassificeringen och de återkommande riskanalyser i reella skydd.

Mål

För att uppnå målet med denna princip ska den egna organisationen ha en modell, exempelvis en säkerhetsarkitektur, som översätter resultatet av informationsklassificeringen och de återkommande riskanalyserna till direkta skyddsåtgärder.

Princip #5 - *att* utifrån återkommande riskanalyser och inträffade incidenter vidta nödvändiga åtgärder för att upprätthålla rätt skyddsnivåer

Syfte & nytta

Återkommande riskanalyser ger en bra grund för att säkerställa rätt nivå av skydd. Riskanalyser bör med fördel utföras med stöd av information från omvärldsbevakning, resultat av tidigare riskanalyser, incidentrapportering samt verksamhetsmässiga- och juridiska krav. Alla identifierade hot och sårbarheter bör klassificeras och riskbestämmas. Risker som bedöms som oacceptabla lindras genom införandet av säkerhetsåtgärder.

Utmaning

Ett införande av rutin för riskanalys och incidenthantering är i ett inledande skede resurskrävande. Det är också av vikt att resultatet från riskanalyserna leder till förbättring. Samma utmaningar omgärdar ett införande av incidenthanteringen.

Mål

För att uppnå målet med denna princip ska den egna organisationen återkommande genomföra riskanalyser och med utgångspunkt från detta vidta lämpliga säkerhetsåtgärder

Princip #6 - *att* tillämpa gemensamma tillitsramverk för att skapa tillit över huvudmannagränser

Syfte & nytta

Ett tillitsramverk kravställer ett antal förmågor, så väl organisatoriska och personella som tekniska och fysiska, i syfte att skapa tillit organisationer i mellan. Ett vanligt scenario är där en part ansvarar för identifiering och behörighetstilldelning, och en annan part tillhandahåller tjänst.

Tillitsramverket förenklar kravställningen i och med att den förlitande parten inte behöver specificera en unik kravbild för varje tjänst utan kan välja en nivå av tillit som står i relation till informationstillgångens skyddsvärde och krav.

Utmaning

Höga krav på tillit ställer direkt höga krav på exempelvis rutiner och efterlevnad vilket kan uppfattas besvärande, inte minst för den som har ett eftersatt informationssäkerhetsarbete. Oavsett tillämpning av tillitsramverk eller ej kvarstår

kravbilden där exempelvis Datainspektionen gör tolkningen av 31 § i personuppgiftslagen att åtkomst till en tjänst över öppna nät, såsom Sjunet och internet, som innehåller känsliga personuppgifter, ska föregås av stark autentisering. Socialstyrelsens författningssamling (SOSFS 2008:14) 2 kap. 5 § gör samma tolkning vid hantering av patientuppgifter.

Mål

För att uppnå målet med denna princip ska den egna organisationen leva upp till de aktuella kraven för en viss tillitsnivå i ett för ändamålet utpekat tillitsramverk.

Princip #7 - *att* koppla informationstillgångar till relevanta tillitsnivåer

Syfte & nytta

Informationstillgångar som är klassificerad i enlighet med princip #3 kan under relativt enkla former, kombinerade med invägd risk och med hänsyn till berörd författningsreglering, kopplas till ett krav på lämplig tillitsnivå. En sådan koppling gör varje val av tillitsnivå enkel och konsekvent.

Kopplingen av informationstillången, med invägd risk och med hänsyn till berörd författningsreglering, gör att varje informationstillgång får rätt nivå av skydd. Här är det rimligt att dels se tvingande kontroller på informationen, dels tillämpningskontroller vid användning av informationen.

Utmaning

Denna princip kräver att både princip #3 och princip #4 är införlivade. Det är ett relativt omfattande arbete att införliva , inte minst ur perspektivet att det är inte bara en engångsföreteelse. Det kräver en fungerande och iterativ process för att nå målet.

Mål

För att uppnå målet med denna princip ska den egna organisationen ange relevanta tillitsnivåer för de informationstillgångar som ska tillgängliggöras.

Princip #8 - *att* ha förmågan att utfärda och/eller konsumera elektroniska identitets- och behörighetsintyg

Syfte & nytta

Inom ett antal branscher och sektorer ses en federativ samverkan som en form av samverkan över huvudmannagränser. För att ingå i en federation krävs att federationens aktuella tillitsramverk följs. I praktiken en översyn av rutiner och processer i identitets- och behörighetshantering. För att ingå i en federation krävs också den tekniska förmågan att utfärda och/eller konsumera elektroniska identitetsintyg. När den federativa förmågan finns är det tämligen enkelt att samverka över huvudmannagränser.

Utmaning

Samverkan över huvudmannagränser innebär så väl organisatoriska och personella som tekniska och fysiska krav vilket kan utgöra ett hinder för samverkan. Detta gäller inte minst för en organisation som har ett eftersatt informationssäkerhetsarbete.

Mål

För att uppnå målet med denna princip ska den egna organisationen uppfylla de normativa kraven för att ingå i en federation, i förekommande fall genom kravställning vid upphandling.

Princip #9 - *att* säkerställa att alla delar i det elektroniska identitets- och behörighetsintyget följer aktuella tillitsramverk

Syfte & nytta

Ett elektroniskt identitets- och behörighetsintyg innehåller ett antal delar som har till uppgift att ge förlitande part ett underlag att ge någon form av tillträde till en informationstillgång. Det elektroniska intyget har stora krav på riktighet och utfärdaren har att se till att identitetsbegrepp, tidsstämpling, signatur och tillitsnivå samt behörighetsstyrande attribut och andra former av attribut är korrekta. Utfärdandet av intyget ska ske i enlighet med det för ändamålet överenskomna tillitsramverket.

Ett enhetligt intyg, utfärdat utifrån överenskommet tillitsramverket, gör det tämligen enkelt att samverka över huvudmannagränser.

Utmaning

Samverkan över huvudmannagränser innebär så väl organisatoriska och personella som tekniska och fysiska krav vilket kan utgöra ett hinder för samverkan. Detta gäller inte minst för en organisation som har ett eftersatt informationssäkerhetsarbete.

Mål

För att uppnå målet med denna princip ska den egna organisationen följa det för ändamålet överenskomna tillitsramverket vid samverkan över huvudmannagränser.

Princip #10 - *att* kravställa federativ förmåga i varje tjänst

Syfte & nytta

Med en federativ förmåga i tjänsten blir det tämligen enkelt att samverka över huvudmannagränser utan säkerhetsmässiga avkall.

Varje ny tjänst som har federativ förmåga kan med mindre insatser, i jämförelse med en tjänst som har egna lösningar för identifiering, behörighet etc, införlivas i befintlig arkitektur och infrastruktur. Sett över en livscykel väntas också administrationen av tjänster med federativ förmåga minska. Exempelvis vid administration av behörigheter.

Användarupplevelsen i en federativ lösning gör ingen skillnad på om en tjänst finns i den egna organisationen eller om den återfinns i en annan organisation. Dessutom erhålls single-signon (SSO) till alla tjänster ”på köpet”.

Utmaning

För en leverantör som ännu inte implementerat en federativ förmåga för identifiering, och i förkommande fall behörighet, kan anpassningsarbetet vara betydande. Vid nyutveckling av en tjänst är det omvänt en besparing att inte behöva bygga in funktioner för olika former av identifiering, autentisering, behörighetshantering etc.

Mål

För att uppnå målet med denna princip ska den egna organisationen kravställa federativ förmåga enligt de normativa kraven för varje ny tjänst som upphandlas.

Uppföljning

Regionen avser att följa upp hur de styrande principerna för samverkan införlivas och tillämpas. Det görs genom en enklare enkätundersökning där alla organisationer som antagit principerna gör en självskattning per princip.

Självskattningen görs enligt följande:

- Principen tillämpas helt - det innebär att principen är en införlivad del i organisationens ramverk, processer eller motsvarande.
- Principen tillämpas delvis - det innebär att principen används från fall till annat där organisationen finner lämpligt, men principen är inte en införlivad del i organisationens ramverk, processer eller motsvarande. Fortsatt arbete krävs för att principen skall införlivas helt.
- Arbete påbörjat för att tillämpa principen - det innebär att organisationen ännu inte tillämpar den, men har för avsikt att tillämpa den och införliva den i organisationens ramverk, processer eller motsvarande.
- Ej tillämpningsbar princip - det innebär att organisationen inte kan tillämpa principen.
- Vet ej

Förvaltning

De styrande principerna för samverkan förvaltas av Region Gävleborg.

Bilaga 1 – Normativa referenser

Princip #1 - *att* ha en antagen informationssäkerhetspolicy med tillhörande riktlinjer

- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet MSBFS 2009:10
- Socialstyrelsens föreskrifter (2008:14)
- Affärsverket svenska kraftnäts föreskrifter (2013:1)
- Ledningssystem för informationssäkerhet SS-ISO/IEC 27001: 2013
- Riktlinjer för styrning av informationssäkerhet SS-ISO/IEC 27002:2013

Princip #2 - *att* ha en utsedd person som leder och samordnar informationssäkerhetsarbetet

- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet MSBFS 2009:10
- Socialstyrelsens föreskrifter (2008:14)
- Affärsverket svenska kraftnäts föreskrifter (2013:1)
- Ledningssystem för informationssäkerhet SS-ISO/IEC 27001: 2013
- Riktlinjer för styrning av informationssäkerhet SS-ISO/IEC 27002:2013

Princip #3 - *att* tillämpa en likvärdig metod och jämförbara nivåer för informationsklassning

- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet MSBFS 2009:10
- Socialstyrelsens föreskrifter (2008:14)
- Affärsverket svenska kraftnäts föreskrifter (2013:1)
- Ledningssystem för informationssäkerhet SS-ISO/IEC 27001: 2013
- Riktlinjer för styrning av informationssäkerhet SS-ISO/IEC 27002:2013

Princip #4 - *att* tillse att resultatet av informationsklassificeringen leder till reella skyddsåtgärder

- Region Gävleborgs förenklade Säkerhetsarkitektur
- Open Security Architecture (OSA)
- Recommended Security Controls for Federal Information Systems and Organizations (SP800-53)
- The Open Group Architecture Framework (TOGAF)
- Zachman Architecture Framework (AF)
- Sherwood Applied Business Security Architecture (SABSA)

Princip #5 - *att* utifrån återkommande riskanalyser och inträffade incidenter vidta nödvändiga åtgärder för att upprätthålla rätt skyddsnivåer

- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet MSBFS 2009:10
- Socialstyrelsens föreskrifter (2008:14)
- Affärsverket svenska kraftnäts föreskrifter (2013:1)
- Ledningssystem för informationssäkerhet SS-ISO/IEC 27001: 2013
- Riktlinjer för styrning av informationssäkerhet SS-ISO/IEC 27002:2013
- Riskhantering för informationssäkerhet SS-ISO/IEC 27005:2008, IDT

Princip #6 - *att* tillämpa gemensamma tillitsramverk för att skapa tillit över huvudmannagränser

- I första hand eLegitimationsnämndens tillitsramverk,
- I andra hand Sambis (samverkan för säkrare e-hälsa) tillitsramverk, eller
- Skolfederationens tillitsramverk.

Princip #7 - *att* koppla informationstillgångar till relevanta tillitsnivåer

- Information technology – Security techniques – Entity authentication assurance framework ISO/IEC 29115
- Kantara Initiative – Identity Assurance Framework, IAF
- Office of Management and Budget, OMB – Memorandum 04-04

Princip #8 - *att* ha förmågan att utfärda och/eller konsumera elektroniska identitets- och behörighetsintyg

- I första hand eLegitimationsnämndens tillitsramverk,
- I andra hand Sambis (samverkan för säkrare e-hälsa) tillitsramverk, eller
- Skolfederationens tillitsramverk.
- SAML implementationsprofilen eGov2
- SAML deploymentprofilen saml2int

Princip #9 - *att* säkerställa att alla delar i det elektroniska identitets- och behörighetsintyget följer aktuella tillitsramverk

- I första hand eLegitimationsnämndens tillitsramverk
- I andra hand Sambis (samverkan för säkrare e-hälsa) tillitsramverk, eller
- Skolfederationens tillitsramverk.

Princip #10 - *att* kravställa federativ förmåga i varje tjänst

- SAML implementationsprofilen eGov2
- SAML deploymentprofilen saml2int