BILAGA 5 - Föreskrifter för Gruppföreträdare

Version: 1.2

Innehåll

1 Inledning

I detta dokument fastställs regler för och krav på Gruppföreträdare i Sambi.

Begreppen Gruppföreträdare, Gruppmedlem och Grupp finns definierade i Bilaga 1 – Definitioner.

1.1 Syfte

Avsikten med Grupper är att underlätta för små organisationer att ansluta sig till Sambi. Gruppföreträdare förväntas erbjuda dem en anslutning till Sambi som uppfyller Sambis säkerhetskrav och säkerställer att tilliten inom Sambi bevaras.

En Gruppmedlem behöver inte ha ett eget ledningssystem för informationssäkerhet utan ska kunna förlita sig Gruppföreträdarens ledningssystem för informationssäkerhet. Gruppföreträdarens ska tillhandahålla instruktioner och rutiner som Gruppmedlemmens personal ska följa. Dessa ska motsvara de instruktioner och rutiner som Gruppföreträdaren tillämpar för sin egen personal inom ramen för sitt säkerhetsarbete.

Gruppföreträdarens ska även följa upp Gruppmedlemmarnas efterlevnad av dessa föreskrifter genom revision och tillsyn.

Identitetsintyg som utfärdas för Gruppmedlemmar kan utfärdas i Gruppföreträdarens namn.

1.2 Krav

I följande kapitel specificeras de krav som ställs på en Gruppföreträdare avseende:

- Funktioner
- E-tjänster
- Avtal
- Hantering av Gruppmedlemmar
- Informationssäkerhetsarbete
- Incidenthantering
- Registerhållning

2 Funktioner

En Gruppföreträdare ska vara Medlem som Användarorganisation i Sambi.

En Gruppföreträdare ska åt sina Gruppmedlemmar tillhandahålla följande Funktioner:

- E-legitimationsutfärdande (koppling till e-legitimationer)
- Attributsutgivning
- Identitetsintygsutgivning

Funktionerna ska vara godkända av Sambis Tillitsgranskningstjänst.

Funktionerna kan ägas och drivas av

- Gruppföreträdaren själv,
- Underleverantör till Gruppföreträdaren eller av
- Betrodd Part i Sambi med relevant avtal med Gruppmedlem.

3 Avtal

En Gruppföreträdare ska ha följande avtal

- Anslutningsavtal för medlemskap i Sambi för rollen som Gruppföreträdare
- Avtal med eHälsomyndigheten avseende anslutning till deras tjänster
- Avtal med sina Gruppmedlemmar

Gruppföreträdaren har för sina Gruppmedlemmars räkning det fulla ansvaret i Sambi som Användarorganisation, inklusive att för sina Gruppmedlemmar upprätthålla ett säkerhetsarbete, hantera incidenter och hålla deras kontaktuppgifter aktuella.

3.1 Avtal mellan Gruppföreträdare och Gruppmedlemmar

Gruppföreträdaren är ansvarig för att ha nödvändiga avtal med sina Gruppmedlemmar som reglerar parternas avtalsförhållande. I avtalet ska Gruppföreträdaren av Gruppmedlemen erhålla de behörigheter och befogenheter som krävs för att Gruppföreträdaren ska kunna leva upp till kraven enligt Anslutningsavtalet inkluderat denna bilaga. Detta avtal ska vara undertecknat av ansvarig firmatecknare eller motsvarande behörighet.

3.1.1 Lagring och arkivering av Gruppföreträdarens avtal med Gruppmedlem

Aktiva och avslutade avtal mellan Gruppföreträdare och Gruppmedlem ska bibehållas och lagras i tio år. Gruppföreträdaren ska på begäran kunna visa upp avtal för Federationsoperatören.

3.1.2 Ändring av Sambis Anslutningsavtal

Om ändring sker av Sambis Anslutningsavtal eller dess bilagor, speciellt Tillitsramverket, som berör Gruppmedlem, ska Gruppföreträdaren meddela Gruppmedlemmen via e-post senast 30 dagar innan ändringen träder i kraft. Meddelandet ska innehålla information om konsekvenserna för Gruppmedlemmen och åtgärder som måste vidtas.

4 Hantering av Gruppmedlemmar

Gruppföreträdare ska ha dokumenterade rutiner för hantering av Gruppmedlemmar ur ett livscykelperspektiv. Detta ska inkludera anslutning av ny Gruppmedlem, revision av Gruppmedlem, spärr av Gruppmedlem samt utträde ur Gruppen.

4.1 Anslutning av Gruppmedlem

Gruppföreträdare ska kontrollera att den sökande är behörig att vara Gruppmedlem i Sambi innan anslutning till Gruppen medges samt att den sökande har tagit del av och omfattas av Gruppföreträdarens informationssäkerhetsarbete enligt punkt 5 nedan.

4.2 Uppföljning av Gruppmedlem

Gruppföreträdaren ska minst årligen följa upp att berörd personal hos Gruppmedlemmen är införstådda med Gruppföreträdarens regler och instruktioner för informations- och IT-säkerhet.

Gruppföreträdaren ska även följa upp Gruppmedlem på förekommen anledning, till exempel vid informationssäkerhetsincidenter.

4.3 Spärr av Gruppmedlem

Gruppföreträdaren ska vid behov kunna spärra enskild Gruppmedlem. Sådan avstängning ska omgående rapporteras till Federationsoperatören. Gruppföreträdare ska ha kriterier och rutiner för spärr av Gruppmedlem.

I kriterierna för avstängning ska ingå:

- upprepade informationssäkerhetsincidenter,
- bristande följsamhet mot Gruppföreträdarens regler och instruktioner för informations- och IT-säkerhet för personal,
- anmärkningar av allvarligare art vid granskning eller annan allvarligare informationssäkerhetsbrist.

Spärr bör föregås av en varning till Gruppmedlemmen.

4.4 Avslut av Gruppmedlemskap

Gruppföreträdare ska meddela Federationsoperatören när Gruppmedlem utträder ur Gruppen.

4.5 Återkommande kontroll av behörig Gruppmedlem

Om antalet anställda hos en Gruppmedlem per den 1 november överstiger det tillåtna antalet enligt avtalsbilaga 1 - Definitioner, ska Gruppföreträdaren omgående meddela Gruppmedlem om avslutande av Gruppmedlemsskap. Avslutande av Gruppmedlemskapet ska efter meddelandet ske inom ett år.

5 Informationssäkerhetsarbete

5.1 Krav och ansvar

Gruppföreträdare är ansvarig för att samtliga Gruppmedlemmars informationssäkerhetsarbete uppfyller Sambis Tillitsramverk, både vid anslutningstillfället och under Gruppmedlemmens hela medlemskap.

Ansvaret omfattar också att säkerställa att det finns ekonomiska och personella resurser med rätt kompetens för informationssäkerhetsarbetet hos Gruppföreträdaren.

De krav Sambi ställer på en Gruppmedlems informationssäkerhetsarbetet för sina Användare är de samma som ställs på samtliga Användarorganisationer. Ansvarig gentemot Sambi är dock den Gruppföreträdaren som Gruppmedlemmen är ansluten till. Gruppföreträdaren ansvarar avseende Sambi för Gruppmedlemmens personal så som om vore dess egen.

Gruppföreträdaren ska bedriva ett systematiskt, formaliserat och riskorienterat informationssäkerhetsarbete som både omfattar Gruppföreträdaren själv och dess Gruppmedlemmar. Informationssäkerhetsarbetet ska uppfylla Sambis Tillitsramverk. Detta innebär bland annat att det ska ta sin utgångspunkt i ett ledningssystem för informationssäkerhet baserat på ISO/IEC 27001.

5.1.1 Instruktioner för personal

Gruppföreträdaren ska tillse att att det finns regler och instruktioner för informations- och IT-säkerhet och att berörd personal hos Gruppmedlemmen tar del av dem. Det kan t.ex. ske genom att tilhandahålla en ”Säkerhetshandbok för användare” eller motsvarande och att medarbetaren tecknar en ansvarsförbindelse efter att ha tagit del av denna.

5.1.2 Riskanalys och internrevion

Gruppföreträdaren ska kunna påvisa att deras riskanalyser och internrevision avseende Sambi är relevanta för samtliga Gruppmedlemmar och dess personal.

Riskanalysen ska syfta till att vid behov motivera insatser för att:

- förhindra eller försvåra för obehöriga att få tillgång till information (sekretess)
- säkerställa att den information som produceras och bearbetas är korrekt, aktuell och fullständig (riktighet)
- bidra till att informationen är åtkomlig vid behov (tillgänglighet)
- säkerställa ursprunget av varje transkation (spårbarhet)

För dessa områden ska organisatoriska, adminstrativa och tekniska skyddsåtgärder vidtas och dokumenteras på ett sådant sätt att det går att kontrollera att en tillfredställande skyddsnivå uppnåtts.

För risker som inte anses vara adekvat hanterade ska förbättringsförslag utarbetas, och i den mån de inte direkt kan införas ska förbättringsåtgärder ha dokumentaras i en aktivitetslista.

Informationssäkerhetsskyddet ska granskas regelbundet. Avvikelser och incidenter ska systematiskt dokumenteras och följas upp, så att erfarenheter från dessa kan tas tillvara som en del av det kontinuerliga förbättringsarbetet. Resultatet av säkerhetsarbetet ska årligen samanställas och redovisas.

5.1.3 Ledningssystem för informationssäkerhet

Gruppföreträdaren ska säkerställa att dessa föreskrifter är kända hos samtliga Gruppmedlemmar.

5.2 Tillitsgranskning av Gruppföreträdare

5.2.1 Initial granskning och slutgranskning

Innan en Gruppföreträdaren godkänns av Sambi ska den ha genomgått en initial Tillitsgranskning med ett godkänt resultat. Den initiala Tillitsgranskningen omfattar både Gruppföreträdarens eget uppfyllande av Tillitsramverket, samt dess rutiner för den kommande hantering av Gruppmedlemar. Den initiala Tillitsgranskningen kan genomföras som ett påplatsbesök hos Gruppföreträdaren.

Efter det att Gruppföreträdarens verksamhet har kommit i gång och minst en Gruppmedlem har anslutits, ska en slutgranskning göras. En granskning ska då göras av hur Gruppföreträdarens rutiner för hantering av Gruppmedlemar tillämpas, samt av de eventuella krav som finns på kompletteringar från den initiala Tillitsgranskningen. Slutgranskningen ska genomföras som ett påplatsbesök hos Gruppföreträdaren.

5.2.2 Årlig återkommande tillitsgranskning

Då Gruppföreträdaren har stor betydelse för tilliten inom federationen, ska en Gruppföreträdare årligen granskas av Sambis Tillitsgranskningstjänst.

5.2.3 Omfattning

En Gruppföreträdare ska tillitsgranskas mot krav A, B, C, D och E i Anslutningsavtalets Bilaga 3 – Tillitsramverket, samt de krav som ställs i denna bilaga.

5.2.4 Vid förändring av tjänsten

Gruppföreträdaren ska utan dröjsmål meddela Federationsoperatören eventuella förändringar i de delar av sin eller sina Gruppmedlemmars verksamhet eller tjänster som omfattas av Tillitsgranskningen och/eller sin förmåga att uppfylla Tillitsramverket. Sambis Tillitsgranskningstjänst har, vid meddelande om förändring, rätt att granska hela eller delar av Tillitsgranskningen om detta bedöms vara nödvändigt för att säkerställa att Gruppföreträdaren och dess Gruppmedlemmar följer Tillitsramverket och dessa föreskrifter.

5.2.5 Kontroll av efterlevnad

Sambis Tillitsgranskningstjänst har rätt att utföra extra granskningar av Gruppföreträdaren. Målsättningen för sådan granskning är säkerställa efterlevnaden av Tillitsramverket och dessa föreskrifter för att:

- Bibehålla en hög tillit till Federationens hantering av Elektroniska identiteter och Attribut.
- Få en bättre helhetsbild av hur Elektroniska identiteter och Attribut hanteras.
- Kunna utvärdera hur effektiv Sambis Tillitsgranskningstjänst är.

Sambis Tillitsgranskningstjänst har rätt att utföra en sådan Kontroll av efterlevnad hos Gruppföreträdaren:

- Om Sambiombud, Medlem, Underleverantör eller Federationsoperatören har skäl att misstänka att Gruppföreträdaren eller dess Gruppmedlemmar inte följer Tillitsramverket eller dessa föreskrifter,
- om Incident har inträffat i enlighet med punkt 6 nedan, eller
- för att med stickprov undersöka hur Gruppföreträdaren eller dess Gruppmedlemmar följer Tillitsramverket och dess föreskrifter.

Gruppföreträdaren ska under Kontroll av efterlevnad vara Sambis Tillitsgranskningstjänst behjälplig och inkomma med de detaljer och uppgifter som behövs.

Kontroll av efterlevnad ska föregås av ett skriftligt meddelande från Federationsoperatören till Gruppföreträdaren med angivande av åberopade skäl senast 14 dagar innan granskningen ska ske. Om Kontroll av efterlevnad ska genomföras hos Gruppföreträdarens Underleverantörer ska meddelandet sändas från Federationsoperatören via Gruppföreträdaren till Underleverantören, i enlighet med Tillitsramverkets krav på Sambianslutnas ansvar för sina Underleverantörer. Kontroll av efterlevnad ska genomföras med hänsyn till behov av sekretess och Sambis Tillitsgranskningstjänst svarar för att erforderliga avtal om sekretess träffas med granskaren.

5.2.6 Kontaktperson vid Tillitsgranskning

Gruppföreträdaren ska både vara sin egen och Gruppmedlemmars kontaktperson gentemot Sambis Tillitsgranskningstjänst.

5.2.7 Konfidentialitet

För att Gruppmedlemmar ska kunna känna förtroende för hanteringen, ska Tillitsgranskningsunderlagen och granskningsresultatet hanteras som konfidentiell information av både Gruppföreträdaren och Federationsoperatören.

6 Krav på Incidenthantering

Med incident menas här alla informationssäkerhetshändelser som hotar sekretessen, tillgängligheten, riktigheten, spårbarheten eller tilliten till de Elektroniska identiteter, Attribut och E-tjänster som används i Sambi.

Kravet på incidentrapportering från Gruppföreträdaren och samtliga Gruppmedlemmar är de samma som normalt gäller för samtliga Sambianslutna.

Detta innebär bland annat att oavsett om Incidenten inträffar hos Gruppföreträdaren eller dess Gruppmedlemmar ska Gruppföreträdaren skyndsamt:

a) informera Federationsoperatören om det inträffade,
b) vidta åtgärder för att återställa förtroende, och
c) bistå Gruppmedlemmen och Federationsoperatören i dess arbete att återskapa förtroendet för identiteter och attribut i Sambi.

En Gruppföreträdare ska ha beredskap att hantera allvarliga Incidenter så att verksamheten påverkas minimalt, omfattande

a) Färdiga krishanteringsrutiner och krisorganisation,
b) Giltiga kontaktuppgifter för incidenthantering
c) Förmåga att informera sina anslutna Gruppmedlemmar

d) Förmåga att hantera problem hos sina Gruppmedlemmar

Om en Incident inträffar hos Gruppföreträdaren eller Gruppmedlem är Gruppföreträdaren införstådd med att denna kan få en varning av Federationsoperatören eller om Federationsoperatören därutöver finner det nödvändigt tillfälligt spärra Gruppföreträdarens medverkan i Sambi (genom dess metadata avlägsnas från metadataregistret). Federationsoperatören äger rätt att permanent spärra Gruppföreträdaren.

För det fall en Incident inträffar har Sambis Tillitsgranskningstjänst rätt att genomföra en Kontroll av efterlevnad enligt reglering i detta dokument.

7 Registerhållning

7.1 Gruppföreträdarens kontaktuppgifter

Gruppföreträdaren ska vid var tid tillhandahålla aktuella kontaktuppgifter åt Federationsoperatören.

Gruppföreträdaren är skyldig att omgående meddela Federationsoperatören eventuella förändringar av dessa uppgifter.

7.2 Gruppmedlemmars kontaktuppgifter

Gruppföreträdaren ska hålla ett aktuellt och uppdaterat register över samtliga Gruppmedlemmar som är anslutna via Gruppföreträdaren. Registret ska innehållande namn, e-postadresser, telefonnummer, postadresser och antal anställda samt annan relevant information.

Gruppföreträdaren ska på anmodan av Federationsoperatören kunna redogöra för vilka Gruppmedlemmar som för närvarande finns och deras kontaktuppgifter.

7.3 Årlig rapportering

Gruppföreträdare ska rapportera antal Gruppmedlemmar och antal anställda per Gruppmedlem till Federationsoperatören. Detta ska göras en gång per år.

Gruppföreträdaren ska senast den 1 december varje år meddela Federationsoperatören både antalet Gruppmedlemmar och antalet anställda per Gruppmedlem per den 1 november samma år. Det meddelade antalet Gruppmedlemmar multiplicerat med medlemsavgiften per Gruppmedlem utgör underlag för det kommande årets fakturerade medlemsavgift för Gruppföreträdarens medlemskap i egenskap av Användarorganisation.

Revisionshistorik

Revisionshistorik			
Ver	Datum	Författare	Kommentar
1.0	2019-01-09	Eva Sartorius	
1.1	2019-05-09	Eva Sartorius	Tagit bort krav på att vara Tjänsteleverantör i Sambi
1.2	2019-11-22	Eva Sartorius	Tagit bort styrgruppen och flyttat ansvaret till Federationsoperatören