Sambi
Samverkan
för säkrare
e-hälsa

Tillitsdeklaration

Version: 2.2
Ska användas vid tillitsdeklaration enligt Sambi Tillitsramverk version 2.1

Innehåll

Denna Tillitsdeklaration avser

Namn organisation/företag

____

Organisationsnummer

____

Ange ert unika versionsnummer för denna Tillitsdeklaration

____

Om detta dokument

Denna Tillitsdeklarationsmall ska användas av nya Sökande till Sambi samt vid uppföljande granskningar av befintliga Medlemmar, Underleverantörer och Sambiombud. Tillitsdeklarationen ska återspegla den faktiska situationen inom organisationen vilket är en förutsättning för ömsesidig tillit inom Sambi.

I detta dokument återfinns kraven från Sambis Tillitsramverk (Sambis avtalsbilaga 3 – Tillitsramverk). Efter kraven finns ledtexter vars syfte är att förklara kraven och förtydliga det svar som ska anges. *Ledtexterna anges i detta typsnitt.*

Den Sökandes svar ska anges i de för ändamålet avsedda svarsrutorna. Svarsrutorna kan expanderas vid behov. När svaret refererar till öppna, för Sambi tillgängliga källor räcker det att ange länken dit. Innehåller svaret referenser till interna källor ska dessa bifogas som dokument till Tillitsdeklarationen.

Termer av speciell betydelse för denna bilaga finns definierade i Bilaga 1 – Definitioner för Sambi v 2.2.

Regelverkets tillämpning

Tillitsramverkets krav är uppdelade i sex avsnitt, vilka är tillämpliga för Användarorganisationer, Tjänsteleverantörer, Sambiombud och Underleverantörer enligt tabellen nedan.

Kapitel i Tillitsramverket	Generella krav	E-legitimations-utfärdare	Attributs-utgivare	Idenitets-intygs-utgivare	Tjänste-leverantör	Sambi-ombud
Användar-organisation	Skall krav	Skall Krav	Skall Krav	Skall Krav	-	-
Tjänste-leverantör	Skall Krav	-	-	-	Skall krav	-
Sambiombud	Skall Krav	Skall Krav	Skall Krav	Skall Krav	-	Skall Krav
Gruppföreträdare	Skall Krav	Skall Krav	Skall Krav	Skall Krav	Skall Krav	-
Under-leverantör	Skall Krav	Valbar	Valbar	Valbar	Valbar	-

En **Betrodd part** är en Användarorganisation, Tjänsteleverantör, Sambiombud, Gruppföreträdare eller Underleverantör som innehar en av Sambi aktuell och godkänd Tillitsgranskning.

Den Sökande

Namn på organisationen

____

Organisationsnummer

____

Ange kontaktperson för innehållet i denna Tillitsdeklaration samt bilagda dokument och refererade källor på internet (kontaktpersonen ska vara densamma som på kontaktblanketten)

Namn

____

Telefonnummer

____

E-postadress

____

Roller som ska granskas

Markera er roll eller era roller som denna Tillitsdeklaration avser.

- ☐ **Användarorganisation;** deklarerar för avsnitt A, B, C och D
- ☐ **Tjänsteleverantör;** deklarerar för avsnitt A och E
- ☐ **Underleverantör till Användarorganisation;** deklarerar för avsnitt A och därefter avsnitt B, C eller D beroende på vad som levereras
- ☐ **Underleverantör till Tjänsteleverantör;** deklarerar för avsnitt A och E
- ☐ **Sambiombud;** deklarerar för avsnitt A, B, C, D och F
- ☐ **Gruppföreträdare;** deklarerar för avsnitt A, B, C, D och E samt skickar med en bilaga om hur Bilaga 5 – Föreskrifter för Gruppföreträdare uppfylls.

Beskriv funktionen

Ge en beskrivning av vilka delar av er verksamhet som omfattas av denna Tillitsdeklaration, samt vilka Funktioner för identitets- och behörighetshantering som ingår. Ange namn på Funktionen om det är möjligt, till exempel ”identitetsutgivning xx”, ”attribututgivning yy” eller ”e-tjänst zz”. Ange vilka Roller inom er organisation som är ansvariga och vilka Roller som berörs av Funktionen.

Del av organisationen

Beskriv vilka delar av er organisation som berörs.

A. Generella krav

Övergripande krav på verksamheten

Krav A.1

Betrodd Part som inte är ett offentligt organ ska drivas som registrerad juridisk person samt teckna och vidmakthålla för verksamheten erforderliga försäkringar.

Beskriv er organisationsform och ert ägarförhållande.

Beskriv försäkring av verksamheten som avses i denna Tillitsdeklaration och deras omfattning. För ett offentligt organ behöver denna fråga inte besvaras.

___

Krav A.2

Betrodd Part ska ha en etablerad verksamhet och vara fullt operationell i alla delar som berörs i detta dokument.

Beskriv inom vilken del av er organisation den för Tillitsdeklarationen aktuella verksamheten hanteras.

___

Beskriv hur länge och i vilken omfattning organisationen arbetat med de områden som avses i denna Tillitsdeklaration.

___

Beskriv hur bevakning sker av befintliga och nya legala krav.

Säkerhetsarbete

Krav A.3

Betrodd Part ska för den Funktion Tillitsdeklarationen avser ha infört ett strukturerat säkerhetsarbete anpassat efter risker och säkerhetsbehov, bestående av:

(a) **Riskanalys** avseende den Funktion som Tillitsdeklarationen avser. Denna ska ta hänsyn till skyddsvärde, befintliga skyddsåtgärder och legala krav. Riskanalysen ska omfatta analys av hot och sårbarheter, samt sannolikhet och konsekvens (skada) på Användare, den egna organisationen, andra Medlemmar och Federationsoperatören. Riskanalysen ska genomföras årligen och leda till en förbättringsplan innehållande rekommenderade säkerhetsåtgärder.

(b) Ett **ledningssystem för informationssäkerhet** (LIS) för Funktionen baserat på ISO/IEC 27001. Säkerhetsåtgärderna ska hantera riskerna enligt riskanalysen för Funktionen.

(c) Genomförd **internrevision** av införandet och efterlevnaden av ledningssystemet för informationssäkerhet (b).

Ledningssystemet för informationssäkerhet och efterlevnaden av de krav som ställs i detta Tillitsramverk ska minst en gång per treårsperiod vara föremål för internrevision, utförd av en till Funktionen oberoende kontrollfunktion.

Beskriv ert strukturerade säkerhetsarbete nedan.

Efterlevnaden av detta krav och er beskrivning är centrala för att visa att organisationen har tillräckligt hög säkerhetsnivå för att övriga Medlemmar ska kunna ha tillit till er Funktion.

- *Riskanalysen ska visa vilka skyddsåtgärder som behövs.*
- *Ledningssystem ska innehålla riktlinjer och instruktioner för hur dessa skyddsåtgärder ska utföras.*
- *Internrevisionen ska säkerställa att detta följs.*

Riskanalysen kan använda den av Sambi publicerade hotkatalogen som inspiration. Riskanalysen ska uppdateras regelbundet, och kan leda till förändringar i ledningssystemet. Internrevisionen ska likaså genomföras regelbundet och alltid leda till en tidsatt åtgärdsplan.

Observera att kravet enbart gäller den tjänst eller funktion som Tillitsdeklarationen avser, inte nödvändigtvis hela organisationen.

Beskriv för riskanalyser hur de planeras, periodicitet, fastställande av kontext, riskbedömning och riskidentifiering, riskbehandling, riskkommunikation och hur säkerhetsregelverket uppdateras.

Beskriv ledningssystemet som följer ISO/IEC 27001. Redovisa eventuell avvikelse från ISO/IEC 27001, och motivera i sådana fall detta. Om er organisation har ett certifierat ledningssystem för informationssäkerhet som omfattar Funktionen som denna ansökan avser, bifoga kopia av detta certifikat i stället.

Beskriv, för internrevisionerna, hur de genomförs, rapporteras och hur avvikelser/förbättringsförslag hanteras. Beskriv även hur revisorn utses och hur kvalitén på internrevisionen säkras.

Beskriv, för förbättringsplanen, hur den beslutas, prioriteras, resurssätts, tidsätts, genomförs och följs upp.

För att visa att krav A.3 uppfylls ska den Sökande uppvisa dokument som styrker att ett strukturerat säkerhetsarbete finns och är anpassat efter riskerna och säkerhetsbehovet.

Resultatet av genomförd riskanalys och internrevision ska uppvisas.

För riskanalysen, ledningssystemet och internrevisionen ska även åtgärdsplaner uppvisas.

Observera att kravet inte nödvändigtvis avser dokumentation över hela den Sökandes organisation och verksamhet, utan enbart avser den tjänst eller funktion som Tillitsdeklarationen avser.

Ange vilka dokument som bifogas för att styrka att ett strukturerat säkerhetsarbete finns och är anpassat efter riskerna och säkerhetsbehovet och vad dessa avser.

För att visa att krav A.3 uppfylls kan den Sökande för känslig information göra sekretessmarkeringar i bifogade dokument eller be om att vid behov få uppvisa ytterligare dokument som styrker att ett strukturerat säkerhetsarbete finns och är anpassat efter riskerna och säkerhetsbehovet.

Kravet på en treårsperiod innebär att en årlig internrevision kan fokusera på enbart en del av verksamheten, så att helheten täcks under perioden. Internrevision ska utföras av en extern part eller annan, oberoende, del av den egna organisationen. Oberoende kan förtydligas med ”har en annan chef”.

Krav A.4

Betrodd part har inrättat en process för incidenthantering i enlighet med de av Federationsoperatören angivna instruktionerna.

Beskriv incidenthanteringsprocessen.

Kryptografisk säkerhet och övrigt skydd mot obehörig åtkomst

Krav A.5

Betrodd Part ska skydda Funktionen mot obehörig åtkomst.

Krav på skydd och nyckelhantering finns i Bilaga 2, Tekniska krav.

Beskriv hur skyddet inklusive nyckelhantering sker, och hur de tekniska kraven i Bilaga 2 uppfylls.

Ansvar för användning av Underleverantörer

Krav A.6

Betrodd part som, i delar eller i helhet, lägger ut utförande av Funktionen på Underleverantör är, oavsett avtalsform, ansvarig för Underleverantörens uppfyllande av kraven i Tillitsramverket.

Beskriv vilka delar av Funktionen som är utlagda till Underleverantörer och beskriv avtalsförhållandena.

Detta krav anger att tilliten inom Sambi ska vara oberoende av om organisationen använder sig av Underleverantörer eller utför Funktionen i egen regi. Samtliga krav ska uppfyllas och redovisas oavsett var tjänsten eller funktionen utförs. Ifall Underleverantörer används ska det för samtliga krav redovisas hur Underleverantörerna uppfyller dem. Detta gäller speciellt det centrala kravet A.3, där riskanalys ska göras hos respektive Underleverantör, ett ledningssystem ska finnas och internrevision ska göras.

Detta krav påverkar således hur samtliga övriga krav ska besvaras.

Beskriv hur eventuella Underleverantörer uppfyller kraven, i den mån detta inte redovisas under respektive krav. När Underleverantören har ett certifierat ledningssystem för informationssäkerhet, bifoga även kopia av Underleverantörens certifikat. Om Underleverantören är en Betrodd Part räcker detta för att visa att kravet är uppfyllt.

Ange de funktioner och kritiska processer som lagts ut på Underleverantörer. Beskriv hur kontroll sker att Underleverantören uppfyller kraven för dessa.

Ange vilka avtal som reglerar utförandet hos Underleverantören och beskriv hur dessa säkerställer att kraven uppfylls. Beskriv även de egna rutinerna för att följa upp Underleverantören.

Handlingars bevarande

Krav A.7

Betrodd Part ska, i tillämpliga delar, bevara

(a) avtal
(b) styrande dokument
(c) handlingar som rör förändringar av uppgifter hänförliga till Användare, Attribut och Metadata och
(d) övrig dokumentation som stöder efterlevnaden av de krav som ställs på denne, och som visar att de säkerhetskritiska processerna och kontrollerna fungerar.

Lista allt material som ska arkiveras därför att det ingår i organisationens tillämpning av Tillitsramverket och ISO/IEC 27001. Beskriv hur det listade materialet identifieras och arkiveras.

___

Krav A.8

Tiden för bevarande ska inte understiga tre år och material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallas från integritetssynpunkt och har stöd i lag eller annan författning.

Beskriv hur det säkerställs att listat material kan tas fram och läsas. Redovisa om avvikelse sker från ovan angiven tid och motivera i sådana fall detta.

___

B. E-legitimationsutfärdare

Krav B.1

E-legitimationsutfärdare ska vara godkänd av Myndigheten för digital förvaltning (DIGG) i enlighet med Tillitsramverket för Svensk e-legitimation eller vara anmäld av annat land enligt EU:s eIDAS-förordning. Dessutom är SITHS godkänt i Sambi fram till 2020-06-30 även utan DIGG:s godkännande.

Beskriv vilka e-legitimationer som kommer att användas

___

C. Attribututgivare

Krav C.1

Informationsinnehållet i Attribut ska vara korrekt, aktuellt samt verifierat mot ursprungskällan.

Hänsyn ska tas till resultatet av riskanalysen avseende vilka Attribut som är viktigast ur säkerhetssynpunkt. Vissa Attribut styr inte behörigheter utan är enbart informativa.

Beskriv hur det säkerställs att Attribut är korrekta. Beskriv även hur Attribut hålls aktuella över tiden. Beskriv vilka verifieringar som görs.

___

Krav C.2

Förändringar av informationsinnehållet i Attribut ska gå att spåra avseende tidpunkt för förändring och vem som utfört förändringen.

Beskriv hur loggning görs, vilket innehåll loggarna har samt hur loggarna säkras från otillbörlig manipulering samt regler och rutiner (ansvar) för uppföljning av innehållet i loggar.

D. Identitetsintygsutgivare

Krav D.1

Betrodd Part som tillhandahåller tjänst för utgivning av Identitetsintyg ska se till att denna tjänst har god tillgänglighet och att utlämnande av Identitetsintyg föregås av en tillförlitlig kontroll av att den angivna Användarens Elektroniska identitet och Attribut är giltiga.

Ange ett tillgänglighetsmått för tjänsten.

Beskriv hur kontroll av Attributens giltighet görs, inklusive vilka attributskällor som används. Ange även hur tjänsten genomför kontroll av den angivna användarens elektroniska identitet (kopplingen mot e-legitimation).

Krav D.2

Tillitsnivå ska anges i identitetsintyget. Hur Tillitsnivå anger och tolkas ska följa specifikation från Myndigheten för digital förvaltning (DIGG).

Ange vilka tillitsnivåer som är aktuella för er. För SITHS gäller tilitsnivå 3.

___

Krav D.3

Lämnade Identitetsintyg ska vara giltiga endast så länge som det krävs för att Användaren ska få tillgång till den efterfrågade E-tjänsten.

Ange giltighetstid för intyg.

___

Krav D.4

Informationen i identitetsintyg ska skyddas mot obehörig åtkomst.

Beskriv krypteringsförfarande.

___

Krav D.5

Identitetsintyg ska utfärdas på ett sådant sätt så att Tjänsteleverantören kan kontrollera att mottagna intyg är äkta.

Beskriv signeringsförfarande.

____

Krav D.6

Identifierade Användares inloggningssession mot intygsutgivningstjänsten ska tidsbegränsas, varefter en ny identifiering av Användaren ska ske i enlighet med D.1.

Beskriv hur länge autentiseringen mot intygsutfärdaren är giltig innan ny autentisering krävs.

____

E. Tjänsteleverantör

Krav E.1

Tjänsteleverantör ska ha en dokumenterad rutin för publicering av Attribut och Tillitsnivåer som används för Tjänstens behörighetskontroll.

En Användarorganisation måste få information om vilka egenskaper deras Användare ska ha för att få åtkomst till hela eller delar av tjänsten. Detta ska återspeglas i krav på kvalité och aktualitet på nödvändiga Attribut.

Beskriv rutinen för publicering av Attribut och Tillitsnivåer och hur Användarorganisationer delges.

____

Krav E.2

Tjänsteleverantör ska skydda Användares identitet och tillhörande Attribut.

Bekräfta och beskriv hur skydd av identiteter och Attribut för Användare sker.

___

Krav E.3

Tjänsteleverantör ska informera Användare om informationen sprids eller används på annat sätt än för behörighetsstyrning.

Beskriv om sådan informationsspridning, intygspropagering eller användning görs, och till vem. Beskriv i så fall hur Användaren informeras om detta.

___

F. Sambiombud

Övergripande krav på verksamheten

Krav F.1

Sambiombud ska ha erforderliga försäkringar samt förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten vidare i minst 1 år.

Beskriv kortfattat hur finansiering och exempelvis försäkringar gör att kravet uppfylls. Notera att detta är en utvidgning av krav A.1. För ett offentligt organ behöver denna fråga normalt inte besvaras.

Tillitsgranskning av anslutna Användarorganisationer

Krav F.2

Sambiombudet ska ha väl dokumenterade rutiner för att säkerställa att anslutna Användarorganisationer uppfyller kraven i kapitel A ”Generella krav” av detta ramverk.

Hänsyn ska tas till att Användarorganisationen utnyttjar Sambiombudets tjänster för E-legitimationsutfärdande, attributhantering och intygsutgivning och därmed följande minskning av de återstående riskerna.

Om Användarorganisationen för sin kravuppfyllnad använder riktlinjer utfärdade av Sambiombudet skall denne säkerställa att dessa följs och uppfylls.

Beskriv noggrant rutinerna för att säkerställa kravuppfyllnaden hos de anslutna Användarorganisationerna, speciellt krav A.3. Visa också hur ombudet säkerställer att dessa rutiner följs för samtliga organisationer. Bifoga dokumentation över relevanta rutiner och

processer, tillsammans med sammanställningar av resultaten av användningen av dessa. Exempel på det senare kan vara antal genomförda anslutningar, antal underkända ansökningar, ofta förekommande problem.

Beskriv och bifoga också de riktlinjer, processer och mallar som ombudet använder gentemot Användarorganisationerna. Visa hur ombudet säkerställer att dessa följs.

Notera att riskerna som Användarorganisationerna ska hantera är relativt få, de flesta risker överförs till Sambiombudet. Detta innebär att Sambiombudet får i motsvarande grad stora krav att visa att speciellt kraven A.3 och F.2 är uppfyllda.

Krav F.3

Sambiombudet ska ha väl dokumenterade rutiner för att tillse att en aktuell Tillitsgranskning finns för Användarorganisationer.

Beskriv och bifoga dessa rutiner. Bifoga också en sammanställning av utfallet av användningen av rutinerna.

Incidenthantering

Krav F.4

Sambiombudet ska ha väl dokumenterade rutiner för hantering av incidenter i den egna verksamheten och hos sina Användarorganisationer. Dessa ska minst omfatta att:

- informera Federationsoperatören om det inträffade,
- vidta åtgärder för att återställa förtroende, och
- bistå Medlemmen i dess arbete att återskapa förtroendet för Elektroniska identiteter och Attribut i Sambi.

Beskriv och bifoga incidenthanteringsrutinen. Bifoga också en sammanställning av utfallet av användningen av denna.