Tillitsdeklaration

Version: 2.0
Ska användas vid tillitsdeklaration enligt Sambi Tillitsramverk version 2.01

Innehåll

Denna Tillitsdeklaration avser

Namn organisation/företag

Organisationsnummer

Ange ett unikt 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.

Ledtexter anges som kursiv grå text och med ett mindre 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 2.01.

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
Under-leverantör	Skall Krav	Valbar	Valbar	Valbar	Valbar	-

Definitioner

En Användarorganisation, Tjänsteleverantör, Sambiombud eller Underleverantör som innehar en av Sambi aktuell och godkänd Tillitsgranskning benäms i detta dokument **Betrodd part**. Andra termer av speciell betydelse för Tillitsramverket finns definierade i Bilaga 1 – Definitioner.

Versionsnummer för denna Tillitsdeklaration

Den Sökande

Namn på organisationen

Organisationsnummer

Kontaktperson för innehållet i denna Tillitsdeklaration inkluderande bilagda dokument och refererade källor på internet (ska vara densamma som på kontaktblanketten).

Namn

Telefonnummer

E-postadress

Den funktion som ska granskas

Markera den funktion 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.

Beskriv funktionen

Ge en kortfattad beskrivning inklusive namnet på funktionen denna Tillitsdeklaration avser.

Del av organisationen

Beskriv vilka delar av organisationen och vilka roller som hanterar funktionen.

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 organisationsform och 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. T.ex. om det är ett ”Förvaltningsobjekt” eller hanteras av en avdelning.

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 tjänst som medlemskapet avser ha infört ett strukturerat säkerhetsarbete anpassat efter risker och säkerhetsbehov, bestående av:

(a) En **riskanalys** avseende tjänsten och dess funktioner. 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.

(b) Ett **ledningssystem för informationssäkerhet** för tjänsten baserat på ISO/IEC 27001 eller motsvarande. Säkerhetsåtgärderna ska hantera riskerna enligt riskanalysen för tjänsten och dess funktioner.

(c) Genomförd **internrevision** av införandet och efterlevnaden av säkerhetsregelverket för tjänsten.

Riskanalys och internrevision ska genomföras årligen och leda till en förbättringsplan innehållande rekommenderade säkerhetsåtgärder.

Efterlevnad av detta krav är centralt för att visa att organisationen har tillräckligt hög säkerhetsnivå för att övriga Medlemmar ska kunna ha tillit till denna.

- *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 tidssatt 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 och ange om det följer ISO/IEC 27001. Redovisa eventuell avvikelse från ISO/IEC 27001, och motivera i sådana fall detta. När en Betrodd Part har ett certifierat ledningssystem för informationssäkerhet som omfattar Tillitsramverket, bifoga även kopia av detta certifikat.

Beskriv för internrevisionerna genomförandet, rapporteringen och hur avvikelser/förbättringsförslag hanteras.

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

Krav A.4

Betrodd Part ska tillhandahålla dokumentation över genomförd riskanalys, ledningssystemet för informationssäkerhet samt genomförd internrevision av efterlevnaden och införandet av säkerhetsregelverket, inklusive aktuell förbättringsplan, avseende tjänsten och dess funktioner.

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.

Krav A.5

Medlem ska inrätta en process för incidenthantering som innefattar vidarerapportering till Federationsoperatören i enlighet med de av Federationsoperatören angivna instruktionerna.

Beskriv incidenthanteringsprocessen.

Granskning och uppföljning

Krav A.6

Ledningssystemet för informationssäkerhet och efterlevnaden av de krav som ställs på Betrodd Part ska under en treårsperiod vara föremål för internrevision, utförd av oberoende kontrollfunktion.

Sambi granskningsgrupp ska genomföra en Tillitsgranskning vid ansökan och därefter minst var tredje år enligt Bilaga 4 - Föreskrifter för Sambis Federationsoperatör. Ett Sambiombud ska granskas årligen enligt bilaga 5 av Sambiombudsavtalet.

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

En ny Tillitsdeklaration ska upprättas vart tredje år.

Beskriv för internrevisionerna planeringen, periodicitet, omfattningen, hur revisorn utses och hur kvalitén säkras på internrevisionen.

Kryptografisk säkerhet

Krav A.7

Betrodd Part ska skydda kryptografiskt nyckelmaterial, omfattande minst signeringsnycklar för

a) metadata
b) identitetsintyg
c) kommunikation

Krav på nyckelhantering ges i Bilaga 2, Tekniska krav.

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

Ansvar för användning av Underleverantörer

Krav A.8

Betrodd part som lägger ut utförande av funktion på Underleverantör är som huvudman ansvarig för Underleverantörens uppfyllande av kraven i Tillitsramverket, oavsett avtalsform, och ska redogöra för hur Underleverantören uppfyller kraven så som om det vore utfört av den Betrodde Parten själv. I denna redogörelse ska Betrodd Part bl.a. redovisa:

(a) hur Underleverantören uppfyller kraven i Tillitsramverket
(b) vilka funktioner och kritiska processer som har lagts ut på Underleverantör och hur Betrodd Part säkerställer att Underleverantören uppfyller kraven för dessa
(c) de avtal som definierar vilka funktioner som har lagts ut, hur kraven uppfylls av Underleverantören samt hur uppföljningen utförs.

Detta krav anger att tilliten inom Sambi ska vara oberoende av om organisationen använder sig av Underleverantörer eller utför 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.

A.8.a 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.

A.8.b Ange de funktioner och kritiska processer som lagts ut på Underleverantörer. Beskriv hur kontroll sker att Underleverantören uppfyller kraven för dessa.

A.8.c 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.9

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 material listat i A.9 identifieras och arkiveras.

Krav A.10

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 enligt A.9 kan tas fram och läsas. Redovisa om avvikelse sker från angiven tid enligt krav A.10, och motivera i sådana fall detta.

Information

Krav A.11

Betrodd Part ska tillhandahålla uppgifter om avtal, villkor samt anknytande uppgifter och eventuella begränsningar i användandet av tjänsten till Användare, Tjänste- leverantörer och andra som kan komma att förlita sig på dennes tjänst.

Bekräfta och ange hur dessa uppgifter tillhandahålls.

Krav A.12

Betrodd Part ska till Federationsoperatören tillhandahålla en Tillitsdeklaration som beskriver hur Betrodd Part uppfyller Tillitsramverket. Dokumentet ska följa av Federationsoperatören angivet format. Till denna ska bifogas efterfrågade dokument enligt detta Tillitsramverk.

Lista de dokument som bifogas utöver de som anges i krav A.4 och vad dessa avser.

Krav A.13

Betrodd Part ska på begäran av Federationsoperatören lämna uppgifter om hur verksamheten ägs och styrs.

Bekräfta detta och beskriv tillvägagångsättet för att få dessa uppgifter.

Krav A.14

Betrodd Part ska på ett tydligt sätt informera sina Användare och Federationsoperatören om villkor för tjänsten vid nyteckning eller ändring av tjänsten. Betrodd Part ska informera Federationsoperatören även vid ändringar av kontaktpersoner, federationsgemensamma Metadata och Attribut.

Bekräfta och beskriv tillvägagångssättet för att aktivt informera användarna om villkoren vid nyteckning eller ändring av tjänsten.

Krav A.15

En Betrodd Part som upphör med sin verksamhet ska informera berörda Användare, Betrodda Parter och Federationsoperatören. Den Betrodda Parten ska hålla arkiverat material tillgängligt i enlighet med A.9 och A.10.

Bekräfta detta och ange vilka förberedelser som finns på plats.

B. E-legitimationsutfärdare

Krav B.1

E-legitimationsutfärdare ska vara godkänd av E-legitimationsnämnden som Utfärdare av Svensk e-legitimation på tillitsnivå 3 i enlighet med

E-legitimationsnämndens Tillitsramverk.

Bekräfta att detta har skett och bifoga godkännande från E-legitimationsnämnden.

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 vilka autentiseringsmetoder som används för att ansluta till Intygsutfärdaren (SITHS, OTP, dosa, annan metod) för att utfärda Identitetsintyg. Beskriv hur kontroll av identitetens och Attributets giltighet görs, inklusive vilka attributskällor som används.

Krav D.2

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.3

Identitetsintyg ska skyddas så att informationen endast är läsbar för den mottagande Tjänsteleverantören och att denne kan kontrollera att mottagna intyg är äkta.

Beskriv krypterings- och signeringsförfarande.

Krav D.4

Identifierade Användares anslutningar 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 att publicera aktuella 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 hur åtkomst och behörighet styrs till erbjuden tjänst med angivande av regler och värden.

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

F.1 Sambiombud ska ha förmåga att bära risken för skadeståndsskyldighet samt förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten 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

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.

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

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.