INTERNET STIFTELSEN

Tillitsramverk för Skolfederation

Senast uppdaterad 2024-05-30

INTERNET STIFTELSEN

1 Inledning

Syftet med detta tillitsramverk är att utgöra grund för tillit mellan Medlemmar avseende användares elektroniska identiteter och behörighetsstyrande attribut, samt att skydda användares personliga integritet. Tillitsramverket specificerar de säkerhetskrav som ställs på Medlemmar.

Vid anslutning till Skolfederation förutsätts Medlemmen arbeta med ett antal uppsatta gemensamma målsättningar för säkerhet och tillit. Detta är påkallat dels ur persondataskyddssynpunkt, men även för att etablera och upprätthålla en allmän tillit mellan Användarorganisationer och Tjänsteleverantörer inom Federationen.

Internetstiftelsen är federationsoperatör och tillhandahåller de gemensamma infrastrukturella tjänsterna för federationen.

Termer med speciell innebörd för Federationstjänsterna finns definierade i *Ordlista för Internetstiftelsens Federationstjänster* och skrivs här med inledande versal.

2 Generella krav

2.1 Informationssäkerhet

Informationssäkerhetsarbetet inom Medlemmens verksamhet ska ledas, styras, utvärderas och utvecklas med stöd av ett Ledningssystem för informationssäkerhet (LIS). Till grund för ett sådant arbete rekommenderas ISO/IEC 27001. Ledningssystemet ska innefatta alla delar i Medlemmens verksamhet som berör dennes medverkan i Skolfederation. De delar i Medlemmens verksamhet som inte berör dennes medverkan i Skolfederation behöver ej ingå i Ledningssystemet. Grundläggande är att informationssäkerhetsarbetet kontinuerligt utvärderas och anpassas till identifierade risker och aktuella verksamhets- och omvärldskrav. Arbetet innefattar organisations- och resursfrågor, samt tekniska och administrativa säkerhetsåtgärder som berör Medlemmens medverkan i Skolfederation. Specifikt ska Medlemmen tillse att informationssäkerhetsarbetet innefattar att:

1. samtliga säkerhetskritiska administrativa och tekniska processer har dokumenterats,
2. roller, ansvar och befogenheter finns tydligt definierade med vid var tid tillräckliga personella och ekonomiska resurser,
3. säkerställa tillräckliga organisatoriska, personrelaterade, fysiska och tekniska säkerhetsåtgärder (säkerhetsföreskrifterna i ISO/IEC 27002:2022 rekommenderas som vägledning för att införa informationssäkerhetsåtgärder),
4. ha en process för riskhantering som på ett ändamålsenligt sätt regelbundet analyserar hot och sårbarheter i verksamheten, och som genom införande av säkerhetsåtgärder balanserar riskerna till acceptabla nivåer,

5. ha en process för Incidenthantering som systematiskt säkerställer kvaliteten i e-tjänsten och att lämpliga reaktiva och preventiva åtgärder kan vidtas för att lindra eller förhindra skada vid inträffade Incidenter.

Medlemmen ska också tillse att de delar av den tekniska driftmiljön som är av betydelse för säkerheten i Skolfederation skyddas fysiskt mot röjande av känsliga uppgifter som följd av t.ex. miljörelaterade händelser, otillåten åtkomst eller andra yttre störningar. Tillträdeskontroll ska tillämpas så att åtkomst till känsliga utrymmen är begränsad till behörig personal, att informationsbärande lagringsmedia och pappersdokument förvaras och utmönstras på ett säkert sätt, samt att tillträde till dessa skyddade utrymmen kontinuerligt övervakas.

2.2 Internkontroll

Efterlevnaden av de krav som ställs på Medlemmen genom detta regelverk ska över en treårsperiod vara föremål för internrevision, utförd av oberoende intern kontrollfunktion, såvida inte organisationens storlek eller annan försvarbar orsak motiverar att revision sker på annat sätt. Dokumentation som stöder efterlevnaden av kraven enligt detta regelverk ska bevaras så länge som det krävs för att säkerställa möjlighet till uppföljning. Material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallas utifrån integritetssynpunkt och har stöd i lag eller annan författning.

2.3 Teknisk säkerhet

Medlemmen ska säkerställa spårbarheten vid all logisk och fysisk åtkomst till känsliga IT-system. Åtkomst ska kunna härledas på individnivå och identifieringen av individen ska ske på ett betryggande och säkert sätt. Elektronisk kommunikation som direkt eller indirekt berör känsliga uppgifter ska skyddas mot manipulation och insyn via starka kryptografiska metoder.

3 Specifika krav för Användarorganisationer

3.1 Identifiering och registrering

Användare inom Skolfederation ska identifieras på likvärdigt sätt som vid inskrivning vid den aktuella skolenheten. Om en användare redan har identifierats vid ett inskrivningsförfarande, och dennes identitet därigenom gjorts känd, får denna relation ligga till grund för identifieringen.

Om det råder ett anställnings- eller uppdragsgivarförhållande mellan användaren och Användarorganisationen, ska denna relation ligga till grund för identifieringen istället för enligt ovan.

Användarorganisationen ska, beaktat reglerna för persondataskydd, föra register över anslutna användare. Registreringen bör innefatta personnummer eller samordningsnummer, samt de uppgifter som i övrigt är nödvändiga för att Användarorganisationen ska kunna tillhandahålla den elektroniska ID-handlingen och utfärda Identitetsintyg.

Användarorganisationen ska kontrollera att de personuppgifter som registrerats är korrekta och fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register. Det är Användarorganisationens ansvar att säkerställa att de Attribut som tillförs en elektronisk identitet är korrekta, fullständiga och aktuella. För alla åtgärder som rör hanteringen av elektroniska identiteter och Attribut ska finnas revisionsspår att följa. Användarorganisationen ska också skyndsamt avregistrera användare och spärra den elektroniska ID-handlingen när relationen med den anslutna användaren upphör.

3.2 Utfärdande av elektronisk identitetshandling

I utfärdandefasen kopplas en elektronisk ID-handling till den tidigare fastställda identiteten. Utformningen av den elektroniska ID-handlingen kan variera beroende på vilka säkerhetskrav som i övrigt är tillämpliga, men gemensamt för samtliga idag förekommande metoder för elektronisk identifiering är att ett stycke konfidentiell information binds till användaren på ett tillräckligt säkert sätt. Detta kan vara ett lösenord eller en uppsättning koder, en kryptografisk nyckel eller en personlig säkerhetsmodul.

Den elektroniska ID-handlingen ska utformas och framställas på ett sätt som gör det osannolikt att någon utomstående kan gissa eller räkna ut den konfidentiella information som ligger till grund för den elektroniska identifieringen, ens på maskinell väg.

Användarorganisationen ska också tillhandahålla en tjänst där användaren kan spärra sin elektroniska ID-handling (spärrtjänst). Tjänsten ska ha god tillgänglighet och Användarorganisationen ska behandla anmälan om spärr skyndsamt. Den Användarorganisation som tillhandahåller elektroniska ID-handlingar inom Skolfederation ska spärra sådana elektroniska ID-handlingar om denne uppmärksammas på eller att det annars kan misstänkas att dessa används eller kan komma att användas i bedrägliga syften.

3.3 Utgivning av identitetsintyg

Användarorganisation som tillhandahåller tjänst för utgivning av Identitetsintyg till förlitande e-tjänster ska följa de tekniska specifikationer som Federationsoperatören från tid till annan föreskriver. Utlämnande av Identitetsintyg ska föregås av en tillförlitlig kontroll av den angivna elektroniska identiteten och den elektroniska ID-handlingens giltighet.

Lämnade Identitetsintyg ska vara giltiga endast så länge som det krävs för att användaren ska få tillgång till den efterfrågade e-tjänsten, samt skyddas så att informationen endast är läsbar

för den avsedda mottagaren och att den som tar emot intyget kan kontrollera att mottagna Identitetsintyg är äkta.

Användarorganisationen ska, beaktat de elektroniska ID-handlingarnas utformning, säkerställa att tekniska säkerhetskontroller införts vid verifiering av användarens elektroniska ID-handling och utfärdande av Identitetsintyg, så att det är osannolikt att utomstående genom avlyssning, återuppspelning eller manipulation av kommunikation, eller genom att gissa koder eller lösenord, kan utge sig för att vara en annan användare än de verkligen är.

4 Specifika krav för Tjänsteleverantörer

4.1 Tolkning av Identitetsintyg

Tolkning av Identitetsintyg ska göras enligt de tekniska specifikationer och på det sätt som Federationsoperatören från tid till annan föreskriver. Detta innefattar att säkerställa att intygen är äkta och är utgivna av en betrodd instans inom Skolfederation.

4.2 Behandling av personuppgifter

Tjänsteleverantören ska vara väl insatt i de rättsliga krav som följer av behandlingen av personuppgifter. Personuppgifter som erhålls via Identitetsintygen får inte användas för andra ändamål än att identifiera användare och fastställa dennes Behörighet.