BILAGA 2

Säkerhetsföreskrifter för Tjänsteleverantörer anslutna till Skolfederation

Version 2.4

Vid anslutning till Skolfederation förutsätts Tjänsteleverantören arbeta med ett antal uppsatta gemensamma målsättningar för säkerhet och tillit. Detta är påkallat dels ur persondataskyddssynpunkt, men också för att etablera och upprätthålla en allmän tillit till de tjänster och lösningar som samverkar inom Federationen.

Föreskrifter för säkerhet och tillit

Drift av E-tjänst inom Skolfederation innebär som regel datoriserad behandling av personuppgifter. Den här behandlingen ska följa reglerna i tillämplig dataskyddslagstiftning, såsom Dataskyddsförordningen (GDPR), såväl som all annan tillämplig lagstiftning. Det är viktigt att säkerställa att personuppgifterna skyddas på ett bra sätt, också för att trygga tilliten till Skolfederation.

Informationssäkerhet

Informationssäkerhetsarbetet inom Tjänsteleverantörens verksamhet ska ledas, styras, utvärderas och utvecklas med stöd av ett ledningssystem. Till grund för ett sådant arbete kan ledningssystemstandarden ISO/IEC 27001 användas. Avgränsningen för ledningssystemet ska innefatta alla delar i Tjänsteleverantörens verksamhet som berör dennes medverkan i Skolfederation. 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 Tjänsteleverantörens medverkan i Skolfederationen. Specifikt bör Tjänsteleverantören tillse att informationssäkerhetsarbetet innefattar att:

1. samtliga säkerhetskritiska administrativa och tekniska processer har dokumenterats och att roller, ansvar och befogenheter finns tydligt definierade,
2. säkerställa att denne vid var tid har tillräckliga personella resurser till förfogande för att uppfylla sina åtaganden,

3. 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,

4. ha en process för incidenthantering som systematiskt säkerställer kvaliteten i e-tjänsten, former för vidarerapportering och att lämpliga reaktiva och preventiva åtgärder kan vidtas för att lindra eller förhindra skada vid inträffade incidenter.

Tjänsteleverantören 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.

Teknisk säkerhet

Tjänsteleverantören 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.

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.

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.

Internkontroll

Efterlevnaden av de krav som ställs på Tjänsteleverantören genom Regelverket 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 från integritetssynpunkt och har stöd i lag eller annan författning.