Bilaga 3c
Informationssäkerhet

Förfrågningsunderlag

Upphandling av IT-stöd för barn- och elevregister inom Skolplattform Stockholm

Box 22049, 104 22 Stockholm. Besöksadress Hantverkargatan 2 F
Telefon: 08-508 33 000 Telefax: 08-508 33 662
registrator.utbildning@stockholm.se
Org. nr 212000-0142

INNEHÅLLSFÖRTECKNING

1 INLEDNING

Denna beskrivning av informationssäkerhetskrav är en del av Avtalet mellan Staden och Leverantören och ska läsas och förstås mot bakgrund av detta.

Syftet med informationssäkerhet är att:
Riktig information ska finnas tillgänglig för behöriga användare på ett spårbart sätt när den behövs.

Denna bilaga beskriver krav på informationssäkerhet för Lösningen.

Krav som rör tillgänglighet till Lösningen återfinns i separat dokument, *Bilaga 4g - Servicenivåer*.

Stadsledningskontoret och utbildningsförvaltningen har styrande dokument inom området informationssäkerhet, vilka som referensinformation återfinns i *Bilaga 6a - Styrande dokument*.

Lösningen kommer att driftas av Staden. Informationssäkerhetskrav gällande IT-driften har därigenom tidigare fastställts i avtal mellan IT-driftsleverantören och Staden.

2 KRAV PÅ INFORMATIONSSÄKERHET FÖR SYSTEMET/TJÄNSTEN

I detta kapitel återfinns krav på informationssäkerhet vad gäller Lösningens egenskaper.

2.1 Identifiering och autentisering

2.1.1 Identifiering och autentisering

Externa användare av Lösningen ska identifieras och autentiseras via Stadens ID-portal, interna via Stadens katalogtjänst, innan åtkomst medges (Se *Stödjande dokument - ID-portalen.zip*).

2.2 Behörighetskontroll

2.2.1 Single sign on

Lösningens behörighetskontrollsystem ska stödja ”Single Sign On” enligt specifikationen SAML 2.0 (Security Assertion Markup Language) och vara integrerat med Stadens identitetshanteringssystem ur vilket användarens identitet, autentiseringsmetod, grupper och roller ska hämtas.

2.2.2 Skolfederation.se

Lösningen ska ha stöd för att konsumera SAML V2-intyg i enlighet med den tekniska specifikation som tagits fram av Skolfederationen (Se *webbplats www.skolfederation.se/teknisk-information).* Lösningen ska efter beslut från Staden tillgängliggöras för Skolplattform Stockholms användare via skolfederation.se.

2.2.3 Behörighetskontrollsystem

Åtkomst till varje del av Lösningen, inklusive skriv- och läsrättigheter till information, ska styras med hjälp av ett anpassningsbart rollbaserat behörighetskontrollsystem. Nivån av åtkomst ska även kunna styras på basis av använd autentiseringsmetod (stark autentisering, engångslösenord, etc.).

2.3 Spårbarhet

2.3.1 Spårbarhet vid ändringar

Användares förändring av information eller inställningar i Lösningen ska loggas med användarens identitet, tidpunkt, och vad som ändrades. Denna historik ska kunna visas i Lösningens användargränssnitt där så krävs.

2.3.2 Spårbarhet för personuppgifter

Användares förändring och läsning av personuppgifter i Lösningen ska loggas med användarens identitet, tidpunkt, och vilka personer och uppgifter åtkomsten gällde. Denna historik ska kunna visas i Lösningens användargränssnitt där så krävs.

2.3.3 Applikationslogg

Lösningens varningar och kritiska fel ska loggas i en fellogg. Prestandainformation, inklusive de mätpunkter som överenskommes med Staden senare, ska loggas i en prestandalogg.

2.3.4 Export av loggdata

Loggarna nämnda här ovan ska minst en gång per dygn exporteras som en textfil. Loggarna ska vara skyddade mot manipulation och ska tillhandahållas på en anvisad plats där de på ett säkert sätt är tillgängliga för Stadens personal.

2.3.5 Tidsstyrning

Lösningens tid ska styras av en valbar tidstjänst (såsom NTP). Systemtid ska vara UTC och tid riktat till användare ska vara svensk normaltid med automatisk omställning till sommartid.

2.3.6 Digital signering av uppgifter

Användare ska kunna, där så tillämpligt, elektroniskt signera en informationsmängd (ex. ett beslut, dokument eller transaktion) genom den signeringstjänst som staden tillhandahåller via en SOA-plattform (Se *Stödjande dokument SOA-plattform.zip*).

2.4 Dataskydd

2.4.1 Behandling av personuppgifter

Behandling av personuppgifter vid tillhandahållandet av Lösningen inklusive eventuell IT-drift ska ske i enlighet med bestämmelserna i personuppgiftslag (1998:204), i vars hänseende Leverantören är Stadens personuppgiftsbiträde.

2.4.2 Sekretessmarkerade personuppgifter

Lösningen ska kunna identifiera och hantera sekretessmarkerade personuppgifter exempelvis på grund av skyddad identitet. Sådana uppgifter ska kunna hanteras enligt särskilda rutiner och regler (Se *Stödjande dokument Personuppgifter.zip*).

2.4.3 Krypterad datakommunikation

Datakommunikation mellan Lösningen och dess användare respektive andra delar av Skolplattformen ska vara skyddad från insyn genom kryptering.

2.4.4 Krypterad lagring på klientenheter

I det fall data lagras på användares mobila eller fasta klientenheter ska den vara skyddad genom kryptering och endast åtkomlig efter autentisering.

2.4.5 Lagring av personuppgifter

Lösningen ska använda det personregister Staden tillhandahåller genom en SOA-plattform, och får i tillägg endast lagra de uppgifter ur personregistret och under den tidsperiod som är helt nödvändigt för Lösningens funktion.

2.5 Säkerhet för webbapplikation

2.5.1 Säkerhet för webbapplikation

De delar av Lösningen som utgörs av webbapplikation ska leva upp till Stadens krav, nivå 1 till 3, gällande utveckling av säkra webbapplikationer (Se *Stödjande dokument Teknisk kravkatalog*.zip).

2.6 Verifiering av säkerhetskrav

2.6.1 Verifiering av säkerhetskrav

Leverantören ansvarar för att innan driftsättning verifiera att säkerhetskraven efterlevs.