Bilaga 3c
Informationssäkerhet

Förfrågningsunderlag

Upphandling av ett helhetsåtagande avseende IT-stöd för pedagogiskt material 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 3

2 KRAV PÅ INFORMATIONSSÄKERHET FÖR SYSTEMET/TJÄNSTEN 4

2.1 IDENTIFIERING OCH AUTENTISERING 4
2.1.1 Identifiering och autentisering 4
2.2 BEHÖRIGHETSKONTROLL 4
2.2.1 Single sign on 4
2.2.2 Skolfederation.se 4
2.2.3 Behörighetskontrollsystem 4
2.3 SPÅRBARHET 4
2.3.1 Spårbarhet vid ändringar 4
2.3.2 Spårbarhet för personuppgifter 4
2.3.3 Applikationslogg 5
2.3.4 Export av loggdata 5
2.3.5 Tidsstyrning 5
2.3.6 Digital signering av uppgifter 5
2.4 DATASKYDD 5
2.4.1 Behandling av personuppgifter 5
2.4.2 Sekretessmarkerade personuppgifter 5
2.4.3 Krypterad datakommunikation 5
2.4.4 Krypterad lagring på klientenheter 5
2.4.5 Lagring av personuppgifter 5
2.5 SÄKERHET FÖR WEBBAPPLIKATION 6
2.5.1 Säkerhet för webbapplikation 6
2.6 VERIFIERING AV SÄKERHETSKRAV 6
2.6.1 Verifiering av säkerhetskrav 6

3 KRAV PÅ INFORMATIONSSÄKERHET FÖR IT-DRIFT 7

3.1 SÄKERHETSORGANISATION 7
3.1.1 Roller och ansvar 7
3.1.2 Utbildning inom informationssäkerhet 7
3.2 SÄKERHETSPROCESSER 7
3.2.1 Process för behörighetsadministration 7
3.2.2 Process för säkerhetsuppdateringar 7
3.2.3 Process för ändringshantering 7
3.2.4 Process för incidenthantering 8
3.2.5 Process för driftövervakning 8
3.2.6 Process för loggning 8
3.2.7 Process för säkerhetskopiering 8
3.2.8 Process för återstart 8
3.2.9 Process för utrangering av datamedia 8
3.3 SÄKERHETSKRAV PÅ IT-DRIFTMILJÖN 9
3.3.1 Krypterad datakommunikation för IT-drift 9
3.3.2 Brandväggsskydd 9
3.3.3 Identifiering och autentisering för IT-driftpersonal 9
3.3.4 Skydd för klientenheter som används av IT-driftpersonal 9
3.4 FYSISK SÄKERHET 9
3.4.1 Fysisk säkerhet 9
3.5 ANALYS, GRANSKNING OCH RAPPORTERING 9
3.5.1 Riskanalys 9

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*.

Framställningen är uppdelad i krav på två delområden:

- informationssäkerhet som rör själva Lösningen, samt
- krav på informationssäkerhet som gäller för IT-driften av Lösningen.

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.

3 KRAV PÅ INFORMATIONSSÄKERHET FÖR IT-DRIFT

Detta kapitel innehåller krav på informationssäkerhet vad avser IT-driften för Lösningen.

3.1 Säkerhetsorganisation

3.1.1 Roller och ansvar

Leverantören ska ha en fastställd och dokumenterad organisation gällande IT- och informationssäkerhet för IT-driften, inklusive tydliga roller och ansvar.

3.1.2 Utbildning inom informationssäkerhet

Leverantören ansvarar för att personal som beräknas bli involverade i IT-driften dessförinnan och sedan minst årligen får information och utbildning om IT- och informationssäkerhet. Utbildningen ska innefatta säkerhetsorganisation, eget ansvar och roll, Stadens säkerhetskrav, samt generellt säkerhetsmedvetande.

3.2 Säkerhetsprocesser

3.2.1 Process för behörighetsadministration

Leverantören ska genom en dokumenterad rutin för behörighetsadministration tillse att personal ges åtkomst till komponenter i IT-driften efter undertecknat sekretessavtal och endast under den tid och i den omfattning som krävs för att ändamålsenligt kunna utföra sina arbetsuppgifter.

3.2.2 Process för säkerhetsuppdateringar

Leverantören ska genom en dokumenterad rutin löpande informera sig om, först testa och sedan applicera säkerhetsuppdateringar för de i IT-driften ingående komponenterna. Kritiska säkerhetsuppdateringar ska appliceras inom 24 timmar.

3.2.3 Process för ändringshantering

Leverantören ska genom en dokumenterad rutin för ändringshantering styra väsentliga ändringar på ett sådant sätt att negativ påverkan på IT-driftens tillgänglighet, riktighet, sekretess och spårbarhet undviks.

3.2.4 Process för incidenthantering

Leverantören ska genom en dokumenterad rutin för incidenthantering styra hur säkerhetsincidenter i IT-driften ska identifieras, rapporteras, hanteras och eskaleras. Vid allvarliga incidenter ska Stadens utpekade kontaktperson omgående informeras. Rutinen ska vara utformad så att den fungerar effektivt med Stadens rutin för incidenthantering vilken bygger på ITIL incident management.

3.2.5 Process för driftövervakning

Leverantören ska genom en dokumenterad rutin och automatiserat stöd för driftövervakning övervaka, detektera och larma vid otillgängliga tjänster, inklusive en funktion för att meddela utvalda personer att tjänsten är otillgänglig samt när den beräknas vara tillgänglig igen.

3.2.6 Process för loggning

Leverantören ska genom en dokumenterad rutin och automatiserat stöd logga och larma enligt standardinställningar i ingående komponenter samt dessutom; alla interaktioner driftpersonal har med Lösningen, förekomst av skadlig kod, lyckade och misslyckade inloggningsförsök, samt slagningar på personuppgifter som sker direkt i operativsystem eller databas. Loggarna ska vara skyddade mot obehörig åtkomst och manipulation.

3.2.7 Process för säkerhetskopiering

Leverantören ska genom en dokumenterad rutin för säkerhetskopiering tillse att information och Lösning säkerhetskopieras dagligen, att kopiorna verifieras, skyddas mot obehörig åtkomst, lagras på annan plats än driftstället, samt är märkta.

3.2.8 Process för återstart

Leverantören ska genom en dokumenterad och årligen testad rutin för återstart tillse att IT-driften utan onödigt dröjsmål kan komma igång igen efter eventuellt avbrott. De årliga testerna ska innefatta fullständigt test av återläsning av säkerhetskopia.

3.2.9 Process för utrangering av datamedia

Leverantören ska genom en dokumenterad rutin tillse att data på datamedia som inte längre används för stadens IT-drift destrueras permanent genom säker överskrivning.

3.3 Säkerhetskrav på IT-driftmiljön

3.3.1 Krypterad datakommunikation för IT-drift

Datakommunikation mellan driftpersonal och IT-driftens komponenter respektive mellan komponenterna ska vara skyddad från insyn genom kryptering.

3.3.2 Brandväggsskydd

Brandväggar, vilka ska ingå i IT-driften, ska vara konfigurerade så att endast sådan trafik som krävs för tjänsternas tillhandahållande och administration tillåts till de i IT-driften ingående komponenterna.

3.3.3 Identifiering och autentisering för IT-driftpersonal

Driftpersonalens åtkomst till de i driften ingående komponenterna ska endast medges efter identifiering och tvåfaktorsautentisering.

3.3.4 Skydd för klientenheter som används av IT-driftpersonal

Klientdatorer inklusive mobila som används av personal för IT-driften ska vara försedda med tidsstyrt (maximalt 5 minuter) automatiskt aktiverat lösenordsskydd eller annan mekanism för att förhindra obehörig åtkomst.

3.4 Fysisk säkerhet

3.4.1 Fysisk säkerhet

Servrar och andra informationsbehandlingsresurser som används i driften ska förvaras i skalskyddade utrymmen med tillträdeskontroller vilka tillser att endast behörig personal tillåts inträde. Nivån på det fysiska skyddet ska i övrigt följa branschnormer för brandskydd och stöldsskydd.

3.5 Analys, granskning och rapportering

3.5.1 Riskanalys

Leverantören ska årligen utföra en riskanalys samt teknisk test av de i IT-driften ingående komponenterna i syfte att identifiera och åtgärda sårbarheter. Resultat och åtgärder som följer av analys och test ska dokumenteras.