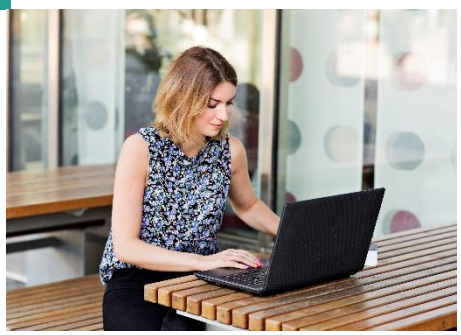
Stockholms stad

Bilaga 3c Informations-säkerhet

Dnr: 220-1874/2017
2018-01-19



Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan 3D
105 35 Stockholm
Växel 08-508 29 000
www.stockholm.se

Innehåll

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 7 - Styrande dokument*.

Framställningen är uppdelad i krav på två delområden:

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

2 Krav på Informationssäkerhet för Lösningen

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

2.1 Identifiering och åtkomstkontroll

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

Lösningen ska tillhandahålla stöd för de autentiseringsmetoder som förekommer inom Stadens ID-portal.

2.1.1 Single sign on

Lösningens identifieringskontrollsystem 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.

2.1.2 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.).

2.2 Spårbarhet

2.2.1 Spårbarhet av händelser

Användarinitierade händelser som in- och utloggningar, skapande, visande och 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.

2.2.2 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.

2.2.3 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.

2.2.4 Export av loggdata

Loggarna nämnda här ovan inom avsnitt 2.2.1 – 2.2.3 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.

2.2.5 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.

2.2.6 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*).

2.3 Dataskydd

2.3.1 Behandling av personuppgifter

Behandling av personuppgifter vid tillhandahållandet av Lösningen inklusive eventuell IT-drift ska ske i enlighet med bestämmelserna i personuppgiftslag (1998:204), samt den allmänna dataskyddsförordningen GDPR som träder i kraft 25 maj 2018, i vars hänseende Leverantören är Stadens personuppgiftsbiträde.

2.3.2 Sekretessmarkerade personuppgifter

Lösningen ska kunna identifiera och hantera sekretessmarkerade personuppgifter exempelvis på grund av skyddad identitet. Sådana uppgifter ska kunna hanteras i samråd med Staden enligt särskilda rutiner och regler (Se *Stödjande dokument Stadsövergripande policy om skyddade personuppgifter*).

2.3.3 Krypterad datakommunikation

Datakommunikation mellan Lösningen och dess användare respektive andra delar av Skolplattformen ska vara skyddad från insyn genom kryptering. Leverantören ska ha rutiner för kryptering där val av algoritmer, protokoll och nyckellängder framgår.

2.3.4 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.

2.3.5 Lagring av personuppgifter

Lösningen ska använda det personregister som tillhandahålls via Stadens katalogtjänst (AD), och får i tillägg endast lagra de uppgifter ur personregistret och under den tidsperiod som är helt nödvändigt för Lösningens funktion. Leverantören ska ha rutiner och funktioner för att permanent radera information som är relaterad till Lösningen.

2.4 Säkerhet för webbapplikation

2.4.1 Säkerhet för webbapplikation

Leverantören ska ha fastlagda och dokumenterade principer och metoder för utveckling av säkra system. Vid webbutveckling ska OWASP:s (www.owasp.org) rekommendationer följas.

Se även *Stödjande dokument Teknisk kravkatalog*.

2.5 Verifiering av säkerhetskrav

2.5.1 Verifiering av säkerhetskrav

Leverantören ska vidta och åtgärda de brister som kan komma att uppdagas samt säkerställer att webbtjänsten inte är sårbar, vad gäller någon av bristerna som nämns i The Open Web-Application Security Project (OWASP):s senast uppdaterade topp tio (10) lista. På begäran av Staden ska Leverantören översända ett granskningsprotokoll, vilket ska godkännas till dess innehåll av Staden där Leverantören visar hur de åtgärdat de brister som beskrivs i OWASP.

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 hantering av testdata

Leverantören ska testa samtliga leveranser i separat testmiljö innan de införs i Stadens tjänst. Testdata ska skyddas och kontrolleras. Testdata ska ej inkludera information som är känslig eller omfattas av sekretess.

3.2.4 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.

3.2.5 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.

3.2.6 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. Leverantören ska även ha funktioner, processer och rutiner för att övervaka och göra analyser avseende kapacitet och prestanda.

3.2.7 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.

3.2.8 Process för säkerhetskopiering

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

3.2.9 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.

3.2.10 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 enligt bästa praxis.

3.2.11 Process gallring och arkivering

Leverantören ska vid behov tillhandahålla metoder för gallring om det påvisas att det finns information som måste arkiveras/gallras.

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 nödvändig 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 enheter 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

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 stöldskydd.

3.5 Analys, granskning och rapportering

3.5.1 Informationsklassificering och risk- och sårbarhetsanalys

Leverantören ska årligen medverka i Stadens informationsklassificering av Lösningen.

Leverantören ska årligen medverka vid risk- och sårbarbetsanalys 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.

Leverantören är införstådd med att Lösningen som efterfrågas i upphandlingen måste uppfylla samtliga Stadens krav på säkerhet och informationssäkerhet enligt Stadens vid var tid gällande riktlinjer och regelverk.

För det fall informationsklassificeringen och riskanalysen visar att ytterligare säkerhetskrav än de som har ställts i Avtalet är nödvändiga för att Lösningen ska uppnå Stadens krav avseende skyddsnivå, åtar sig Leverantören att anpassa Lösningen efter dessa krav.

Om Leverantören kan visa att Stadens informationsklassificering av Lösningen och tillhörande risk- och sårbarhetsanalys innebär väsentligt högre kostnader för Leverantören, ska Parterna då

överenskomma om skälig ytterligare ersättning till Leverantören för uppfyllande av dessa krav. Vid oenighet mellan Parterna gäller Stadens uppfattning om vad som är skälig ytterligare ersättning.