Säkerhetskrav

ÅJ Distribution AB, Ny kundwebshop

Bilaga 8

ÅJ Distribution AB
Arrendevägen 36
163 44 Spånga
Upphandling@ajdistribution.se
www.ajdistribution.se

Kontaktperson
Elisabeth Matzén Beckert
073 885 27 28

1. Säkerhetskrav

Leverantören ska bedriva ett aktivt säkerhetsarbete och följa etablerad branschpraxis och standardmetoder för utvecklingsprojekt, och med den fackmannamässighet, effektivitet och omsorg som Beställaren kan förvänta sig av ett företag med gott anseende i branschen.

2. METODISKT SÄKERHETSARBETE

2.1 Leverantören ska löpande och i samråd med Beställaren arbeta för att leveransen i alla lägen följer de aktuella lagar, förordningar, regler och föreskrifter som ställs på Beställarens verksamhet.

2.2 Leverantören ska upprätta avtal om sekretess. Sekretessavtal ska upprättas då konfidentiell information kan komma att utbytas. Sekretessen omfattar även anställda hos leverantören, konsulter hos leverantören, de personer leverantören sätter i sitt ställe eller andra personer som kan komma i kontakt med sådan konfidentiell information hos leverantören.

Denna förbindelse gäller utan begränsning i tid och även efter att samarbetet mellan parterna i övrigt har upphört.

Med konfidentiell information avses sådan information om Beställaren och deras verksamhet som avser alla typer av affärshemligheter, kunskap eller upplysningar, vare sig dessa är dokumenterade eller inte, vars avslöjande kan komma att skada Beställaren.

Med icke-konfidentiell information avses
- sådan information eller upplysning som är allmänt känd och som kommer part tillhanda på annat sätt än genom informationsutbyte parterna emellan,

- sådan information eller upplysning som part hade redan innan avtalet ingicks, eller
- sådan information som part har fått från utomstående utan att vara bunden av sekretess gentemot denne.

Leverantören förbinder sig att inte för utomstående, såsom t.ex. fysiska eller juridiska personer eller myndigheter, avslöja information som erhållits genom parternas samarbete.

2.3. Leverantören ska se till att säkerhetsarbetet utförs på ett effektivt och resurssnålt sätt samt att säkerhetsarbetet är möjligt att följa upp och granskas av Beställaren eller av en opartisk extern revisor.

2.4 Leverantören ska testa samtliga leveranser i separat testmiljö innan de införs i Beställarens tjänst. Testdata ska skyddas och kontrolleras och får inte innehålla information som är känslig eller omfattas av sekretess.

3. LÖPANDE SÄKERHETSARBETE

Leverantören ska:

3.1 Övervaka, rapportera och begränsa effekter av säkerhetsincidenter.

3.2 Genomföra sårbarhets- och penetrationstester efter beställning.

3.3 Löpande följa upp vilka personer som har olika former av administratörsrättigheter samt rapportera till Beställarens kontaktpersoner hur många och vilka dessa personer är.

3.4 Ha en kontinuerlig översyn av skydd mot säkerhetsbrister och obehörig åtkomst.

3.5 Genomföra kapacitetsplanering och riskanalys för kapacitet.

3.6 Genomföra interna och av Beställaren begärda revisioner av säkerhetsarbetet.

3.7 Leverantören ska proaktivt och vid förfrågan bistå med stöd och rekommendationer inom säkerhetsområdet gällande Tjänsten och nyttjandet av denna.

4. GRANSKNING OCH REVISION

4.1 Leverantören ska efter beställning tillåta säkerhetsgranskning, säkerhetsrevision samt logguppföljning av Beställaren eller av oberoende part. Beställaren ska ta del av granskningens sammanfattning och Leverantörens tidsplan för åtgärder.

5. KRAV PÅ INFORMATIONSSÄKERHET

5.1 Informationen i tjänsten ska hanteras och lagras inom EU/EES av en fysisk eller juridisk person som på inget sätt, direkt eller indirekt, omfattas av lagstiftning i tredjeland.

6. SKYDD

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

6.2 Leverantörens uppgradering, konfiguration och uppdatering av Tjänsten ska alltid kunna ske utan dataförlust och funktionalitetsförlust.

7. SKADLIG KOD

7.1 Samtliga komponenter som skapas och ingår i Tjänsten ska på lämpligt sätt skyddas från skadlig och ondsint kod (skadeprogram). Antivirus ska ses som ett grundskydd och ingå i Uppdraget.

8. SÄKRA SYSTEM

8.1 Leverantören ska verifiera och begränsa den mjukvara som får installeras och exekveras inom den levererade Tjänsten.

8.2 Källkod framtagen i egen utveckling ska skyddas för obehöriga förändringar gentemot den godkända och fastställda versionen.

9. KRYPTERING

9.1 I den Tjänst som exponeras över öppna nät ska transport av data skyddas med kryptering på lämpligt sätt. Endast protokoll som erbjuder hög säkerhet enligt branschstandard ska användas.

9.2 Leverantören ska ha rutiner för kryptering där val av algoritmer, protokoll och nyckellängder samt hantering av krypteringsnycklar framgår.

10. SÄKERHETSUPPDATERINGAR

10.1 Leverantören ska ha processer och rutiner för att identifiera och installera säkerhetsuppdateringar på samtliga komponenter som skapar den Tjänst som Beställaren använder hos Leverantören.

10.2 Leverantören ska ha en process för att prioritera uppdateringar för att exempelvis kunna bedöma om en uppdatering måste installeras omedelbart eller om den kan vänta till nästa servicefönster.