Avima – säkerhet

Avima är en tjänst som är tillgänglig dygnet runt alla dagar. Många av våra kunder lagrar konfidentiell och kritisk information i tjänsten. För att klara av det ställs höga krav på tillgänglighet och säkerhet. I det här dokumentet beskriver vi översiktligt hur vi hanterar och arbetar med dessa frågor.

Driftsmiljön
Avimas driftspartner Axians ansvarar för hela produktionsmiljön. Axians är en ledande aktör i Sverige och har varit Avimas driftspartner sedan år 2008. Axians är certifierade enligt IS0 27001.

Driftsmiljön, dvs. Internetanslutning, brandväggar, lastbalansering, webbservrar, databasservrar, applikationsservrar, filservrar, routrar, switchar etc., är fullt ut redundant för att minimera risken att tjänsten inte är åtkomlig när någon del i miljön inte fungerar. Miljön är uppsatt på två olika geografiska platser för att kunna upprätthålla drift i det fall en en större katastrofhändelse inträffar.

Övervakning av miljön och åtgärder görs dygnet runt, alla dagar. Driftsmiljön är belägen i Stockholm, Sverige.

Den fysiska säkerheten (inpassering, strömförsörjning, brandskydd, klimatkontroll) finns beskriven i mer detalj i dokumentet ”Avima – fysisk säkerhet”, som finns att ladda ner på www.avima.se.

Kommunikation
All kommunikation mellan användarens dator och Avima sker via en krypterad och säker anslutning (SSL). De SSL certifikat som Avima använder är utfärdade av Thawte. Minst 128-bit SSL kryptering och 2048-bit RSA nyckel används.

Internetanslutning
Avima använder en redundant Internet anslutning med hög bandbredd och med minst två operatörer. En dubblerad nätinfrastruktur gör att vi kan garantera hög tillgänglighet på Internet anslutningen.

Tillgänglighet
Avima säkerställer en hög tillgänglighet till tjänsten genom flera förebyggande åtgärder:

- Driftspartner som genom övervakning och åtgärder säkerställer att allt fungerar dygnet runt alla dagar.
- Redundant Internetanslutning.
- Redundant driftsmiljö.
- Geografisk redundans.
- Lastbalansering.

Datalagring
Avima gör många åtgärder för att skydda kundernas
information när den lagras:

- Driftsmiljön är placerad i en byggnad med hög fysisk säkerhet.
- Övervakning av aktivitetsloggar för att identifiera icke förväntad aktivtet.
- Lösenord krypteras.
- Dokument krypteras. (Tillval)
- Avimas personal har alla undertecknat ett sekretessavtal som förbjuder anställda att använda eller utlämna konfidentiell information.

Användaridentifiering
En användare kan endast komma åt den information som hon har behörighet till. I systemet anges vem eller vilka som ska ha åtkomst till en viss modul och vad man ska få göra med ett visst objekt, t.ex. ett dokument.

Alla användare har ett användarnamn och ett lösenord. Som användarnamn används användarens e-postadress, vilken måste verifieras innan det kan användas.

Avima kan erbjuda koppling till AD via SAML 2.0.

Spårbarhet
Aktiviteter i systemet kan loggas och läsas i efterhand. Till exempel loggas läsning och ändringar av dokument. Denna logg är tillgänglig för kundens administratörer. Samtliga användares inloggningar loggas och finns åtkomliga för kundens administratörer.

Integritet
Avima upprätthåller en stark integritetspolicy för att skydda kundernas och användarnas data. Avima äger inte kundernas data och delar den inte heller med tredje part. Avimas personal och partners har skrivit på sekretessavtal. Endast ett fåtal individer i personalen har tillgång till våra produktionssystem.

Intrångsdetektion
Avimas driftspartner övervakar brandväggar och internetaccess dygnet runt med övervakningsverktyg och med IDS-system (Intrusion Detection System).
Övervakningen sker i realtid dygnet runt, inkluderande analys från Symantecs Security Operations Centers (SOC).

Backup och återställning
Fullständig backup tas en gång per dygn och lagras på annan geografisk plats. Inkrementell backup görs frekvent under hela dygnet. Alla data speglas kontinuerligt mellan servrar och är tillgänglig i det fall en störning uppstår.

Återställningstester genomförs kontinuerligt i syfte att säkerställa att det fungerar som det ska. De backuper som görs har det primära syftet att möjliggöra en fullständig återställning av system och data.

Cookies
I Avima används cookies för att spara användarnamn, lösenord och språk, så att användaren inte behöver ange denna information vid varje inloggningstillfälle.

Lösenordssäkerhet
Användarens lösenord kan endast anges av användaren själv. Lösenord lagras krypterat.

Som standard gäller att lösenordet ska utgöras av minst 8 tecken, varav minst ett specialtecken. Som tillval finns möjlighet att ange egna krav på användarnas lösenordskomplexitet samt en tvåstegsinloggning där den ordinarie inloggningen kompletteras med engångsgkod via SMS eller e-post. Om man förlorat sitt lösenord kan man återställa det genom att ange sin e-postadress och man erhåller då ett mejl med länk för återställning.

Inloggning sker alltid via en krypterad och säker anslutning (SSL). Vid för många misslyckade inloggningsförsök blir användaren tillfälligt utlåst under en viss tid.

För att minska risken att någon obehörig får tillgång till information i systemet blir användare automatiskt utloggade efter en viss tids inaktivitet.

Utökad inloggningssäkerhet
För de kunder som har särskilda krav finns flera möjligheter att konfigurera en utökad inloggningssäkerhet genom anpassade krav på lösenord och inloggning.

- Begränsa inloggning till fördefinerade IP-adresser.
- Tvåstegsinloggning, dvs. man måste också ange ett engångslösenord som användaren får skickat till sig som SMS eller via e-post.
- Valbar lösenordskomplexitet.
- Restriktion mot användning av tidigare använt lösenord.
- Krav på att nytt lösenord anges efter en viss tid.
- Möjlighet att stänga av funktionen att spara inloggningsuppgifter till nästa inloggningstillfälle.

Om Avima

Avima är en plattform som är utvecklad för att stödja projektledare och projektchefer inom bygg- och anläggningsprojekt. Med Avima kan du enkelt hålla koll på alla beslut som fattas, säkerställa att rätt dokumentversioner är tillgängliga, och hantera all nödvändig kommunikation för att underlätta effektivt samarbete. Detta hjälper till att spara tid, pengar och resurser, och säkerställer att alla involverade arbetar mot samma mål genom hela projektets livscykel, från tidigt skede till förvaltning.