Informationssäkerhet – Visma Draftit AB

Senast ändrad 2022-05-12

Innehåll

1 Vår informationssäkerhet

Draftit arbetar för att hålla hög nivå på dataskydd och att uppfylla kraven i GDPR för det data våra kunder anförtror oss.

Detta görs genom löpande strategiskt och operativt förbättringsarbete av rutiner, interna styrdokument, medvetenhet, säkerhetskontroller av vår utvecklade mjukvara och våra driftmiljöer.

2 Underleverantörer

För drift och viss utveckling använder vi underleverantörer. Vi har tecknat biträdesavtal enligt GDPR med dessa där det är nödvändigt, och har också separata sekretessavtal med dem.

3 Driftmiljöer

Vår leverans består av två delar. En mer traditionell med servrar i datacenters. Den andra delen är baserad på molntjänster. Dessa är etablerade och lokaliserade inom EU/EES.

Vår inloggning för slutanvändare hanteras i molntjänst, dock lagras inget användardata där. Se punkt 3.1 - 3.3 för mer information runt lagring av denna information.

De delar som hanteras i molntjänster är Visselblås Incident samt våra Expertprodukter. Där körs all kod i moln, och även databaser för dessa produkter ligger i molntjänster. Lagringen är redundant uppbyggd med replikering över flera regioner. Utöver redundansen görs också löpande backuper på databaserna som en extra säkerhetsåtgärd.

För övriga produkter gäller informationen nedan i avsnitt 3.1 till 3.3.

3.1 Datacenter

Vår driftpartners datacenter är placerat i Sverige.

Datacentret uppfyller moderna krav på kontroll av fysisk åtkomst, brandskydd, UPS:er, övervakning, brandväggar, antivirus, löpande uppdateringar etc.

Vår driftpartner är certifierad enligt ISO 9001, 14001 samt 27001.

Driftmiljön hos vår partner är redundant uppbyggd och helt isolerad från deras andra kunders miljöer genom att vi har egna dedicerade databas- och applikationsservrar samt separat nätverkssegment.

Lokalerna uppfyller säkerhetskrav enligt: SSF 130:6, larmklass 2, SSF 200:3 skyddsklass 2 för mekaniskt inbrottsskydd, samt uppfyller lägst klass 3 i SS3522. För brandlarmsinstallationer följs Svenska Brandskyddsföreningens rekommendationer (SBF 110:6)

3.2 Backup

En full backup av våra databaser görs på dygnsbasis. Därutöver görs också transaktionsbackup löpande varje timme.

Återläsning ska enligt SLA påbörjas inom 1 timme.

Backup görs till ett från driftmiljön geografisk åtskilt datacenter, även det beläget i Sverige.

Backupen vi gör är på systemnivå, den kan inte användas för att återställa ändringar som gjorts av användare i enskilda produkter.

3.3 Drift och underhåll

Vi har enligt avtal med driftleverantören en garanterad tillgänglighet på 99,9% för driftdelarna.

Tillgänglighet för våra tjänster till slutanvändare är ca 99 %. Service och underhåll förläggs till kvällar och helger.

Draftit och driftleverantören arbetar tillsammans med löpande förbättringar av drift och övervakning för att så långt det är möjligt förekomma problem och incidenter.

4 Informationssäkerhet

4.1 Övergripande

Kommunikation klient/server sker via https/TLS.

Kryptering av lösenord och annat känsligt data i databaserna görs med hjälp av moderna standardalgoritmer.

Rollstyrning för åtkomst till våra applikationer och deras funktioner.

Högre krav på lösenordskomplexitet för roller med högre behörigheter.

Loggning vid förändring av kunddata.

Möjlighet att koppla på tvåfaktorsautentisering.

Återkommande penetrationstester.

Interna rutiner och utbildning för att motverka social engineering och liknande.

I utvecklingsarbetet för våra applikationer lutar vi oss emot säkerhetsbranschstandard definierad av OWASP (https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project).

Internt ger vi endast behörighet att läsa information till de anställda som absolut behöver åtkomst för att utföra sina arbetsuppgifter. Det är teknisk personal som ansvarar för drift, underhåll och utveckling, innehållsredaktörer, innehållsadministratörer samt personal som jobbar med kundkontakt och kundsupport. Även våra partners kan ha tillgång till information i detta avseende.

Alla lyder under tystnadspliktsförbindelse, och samtliga utbildas grundligt innan man kvalificeras för arbete med åtkomst till kunddata.

4.2 Inloggning och lösenord

Användarkonton låses efter upprepade misslyckade inloggningsförsök.

Vi erbjuder anpassade lösenordsregler som kan sättas upp enligt önskemål. Det som kan specificeras är antal siffror, antal specialtecken, minsta längd och krav på tvåfaktorsautentisering.

Alla användare med personligt konto kan välja att aktivera tvåfaktorsautentisering i "Min profil". Väljer man att koppla på anpassade lösenordsregler kan man dessutom tvinga sina användare att nyttja det.

Vår lösning bygger på att man använder sin telefon för att via en app generera en säkerhetskod som anges vid inloggning.

4.3 Användarkonton

När ett nytt konto skapas skickas ett registreringsmail till användaren med en länk för val av lösenord. Om användaren glömmer sitt lösenord kan lösenordet återställas, ett mail skickas då till användaren med en länk för återställning av lösenord.

Bägge dessa typer av mejl är giltiga endast under en begränsad tidsperiod.

5 Support

Draftit har två supportnivåer:

Supportnivå 1 bemannas av våra supportspecialister inom CS (Customer Success), som skall identifiera incidenten, öppna ett incidentärende och initiera åtgärd, samt hantera incidenter som kräver djupare kompetens.

Supportnivå 2 bemannas av våra utvecklare. Supportnivå 2 är sista ledet för eskalering och för åtgärd av en incident.

Processflödet för incidenthantering följer ITILs modell för IT Service Management:

En användare ringer eller skickar ett e-postmeddelande till CS för att rapportera en incident.

Ett incidentärende registreras.

CS bekräftar med ett e-mail till användaren/kontaktpersonen att incidenten är registrerad.

Diagnos av incidenten genomförs, felsökning eller eskalering sker.

Om supportteknikern som har tagit emot ärendet själv kan åtgärda det, så tilldelar supportteknikern ärendet till sig själv, åtgärdar det samt meddelar och verifierar funktionen med användaren.

Om inte supportteknikern kan åtgärda ärendet eskaleras ärendet till supportnivå 2 för vidare hantering.

Draftit har även daglig mätning av följande parametrar för att hålla högsta möjliga kvalitet på supporten:

- Svarstid
- Samtalsregistrering
- Åtgärdstid
- Antal samtal per månad
- Genomsnittlig samtalslängd
- Nivå på support och teknikernas kompetens