Svenska kyrkan

Bilaga nr 6

Informationssäkerhetsbilaga - inbegripet tekniska och organisatoriska säkerhetsåtgärder

Kraven på leverantören

Följande krav gäller för Leverantören samt Leverantörens underleverantörer inklusive konsulter som bidrar till utvecklingen av Svenska kyrkan med affärsexpertis och som kommer att få tillgång till, hantera eller lagra information.

Syftet med säkerhetskraven

I denna bilaga fastställs krav för säkerhetsåtgärder och förfaranden för skydd av känslig information som hanteras av Leverantören på uppdrag av Svenska kyrkan. Kraven beskriver nödvändiga organisatoriska och tekniska säkerhetsåtgärder som Leverantören ska implementera vid tillhandahållandet av tjänster till Svenska kyrkan eller produkter där Leverantörer har åtkomst till Svenska kyrkans informationstillgångar.

Svenska kyrkan förväntar sig att de organisatoriska och tekniska säkerhetsåtgärder som beskrivs i säkerhetskraven implementeras som en del av Leverantörens system för hantering av informationssäkerhet (ISMS) där policyer, riktlinjer och instruktioner ytterligare beskriver hur Leverantören, Leverantörens anställda och Leverantörens underleverantörer ska hantera Svenska kyrkans informationstillgångar.

Säkerhetskraven fastställer miniminivån för godtagbart skydd av information som hanteras av Leverantören för Svenska kyrkan.

Samtliga avvikelser från säkerhetskraven i denna bilaga ska dokumenteras och godkännas av Svenska kyrkan.

Tillämpning av säkerhetskrav

Kraven som anges i bilagan ska gälla under hela perioden som Leverantören tillhandahåller tjänster till Svenska kyrkan och så länge som Leverantören eller Leverantörens underleverantörer lagrar eller hanterar Svenska kyrkans information.

Uppfyllande av säkerhetskrav

Leverantören och Svenska kyrkan ska regelbundet (minst en gång per år) diskutera nödvändiga åtgärder som Leverantören ska vidta för att säkerställa att kraven i denna bilaga uppfylls. Om Svenska kyrkan begär det ska Leverantören i god tro lämna ett skriftligt uttalande som bekräftar omfattningen av Leverantörens uppfyllande av kraven i denna bilaga.

Leverantören ska kunna redovisa dokumentation som stödjer Leverantörens påståenden avseende uppfyllandet av överenskomna krav som beskrivs i denna bilaga.

Leverantören åtar sig att lämna in nödvändig dokumentation till Svenska kyrkan enligt överenskommelse eller på begäran.

Rätt till att revidera

Under avtalets löptid, dock högst en gång per år (om inte omständigheterna motiverar ytterligare granskning enligt nedan), får Svenska kyrkan granska Leverantörens uppfyllande av de säkerhetskrav som överenskommits i denna säkerhetsbilaga. Svenska kyrkans rätt att granska Leverantörens interna dokumentation omfattar, men ska inte begränsas till, policys, riktlinjer, rutiner, instruktioner och protokoll som rör informationssäkerheten i de tjänster som tillhandahålls.

Oberoende av ovanstående överenskommer parterna att Svenska kyrkan när som helst får genomföra en revision vid

(1) utredning avseende påstående om felaktig hantering, bedrägeri eller bedragande aktivitet av potentiellt brottslig karaktär

(2) när Svenska kyrkan rimligen anser att en revision är nödvändig för att åtgärda ett betydande operativt problem eller problem som utgör ett hot mot Svenska kyrkans verksamhet eller informationssäkerhet.

Svenska kyrkan har rätt att med 15 arbetsdagars varsel få tillgång till relevant dokumentation och vid behov genomföra fysiska besök på plats.

Konsekvenser

Om Svenska kyrkan vid en granskning, eller av andra skäl, identifierar avvikelser i Leverantörens interna kontroll eller att hanteringen av Svenska kyrkans information avviker från de krav som uttrycks i denna säkerhetsbilaga, ska Leverantören vidta lämpliga åtgärder för att korrigera dessa avvikelser, antingen omedelbart efter upptäckt eller inom rimlig tid därefter. Leverantören ska skriftligen informera Svenska kyrkan om de åtgärder som vidtagits för att korrigera avvikelser.

Frågeformuläret

Frågeformuläret som följer på sidorna 4–9 ska besvaras av Leverantören vid offertförfrågan eller vid annan tidpunkt. Denna Bilaga inklusive de svar som lämnats av Leverantören kommer att bifogas och utgöra del av Avtalet mellan Leverantören och Svenska kyrkan.

Bifoga relevant dokumentation och information

Enligt rubrik “Uppfyllande av säkerhetskrav” ska leverantören ange eventuell ISO-certifiering eller motsvarande, samt bifoga informationssäkerhetspolicy eller annan relevant stödjande dokumentation.

Svaren i frågeformuläret nedan ska innehålla en utförlig beskrivning av hur respektive säkerhetsåtgärd utförs av Leverantören. För att en bedömning ska kunna göras är det inte tillräckligt att enbart hänvisa till en eventuell certifiering.

Organisatoriska säkerhetsåtgärder

	Säkerhetsåtgärd	**Leverantören säkerställer åtgärden genom att- ange svar nedan**
1. Hantering av resurser och tillgångar	Leverantören ska ha en förteckning över all information och alla it-resurser som används för att hantera Svenska kyrkans information. Förteckningen ska dessutom innehålla uppgifter avseende alla underleverantörer, inklusive deras kontaktuppgifter, som hanterar Svenska kyrkans information. Leverantören är ensam ansvarig för att underhålla och uppdatera datainventeringen samt för att rapportera betydande förändringar i hanteringen och förvaltningen av Svenska kyrkans information.	
2. Roller och ansvar	Samtliga anställda hos Leverantören och anställda hos underleverantörer som har tillgång till information från Svenska kyrkan ska ha tydligt definierade roller och ansvarsområden. Rollerna ska ha formellt fastställda åtkomsträttigheter till information som bygger på principerna ”lägsta behörighet” (least privilege) och ”nödvändig åtkomst” (need to know). Rollerna och motsvarande åtkomsträttigheter ska ses över regelbundet (minst en gång per år) och ligga i linje med de fastställda ansvarsområdena.	
3. Styrning av åtkomst	Regler för styrning av åtkomst ska dokumenteras för all hantering av information som rör Leverantörens hantering av Svenska kyrkans information. Reglerna ska baseras på principerna ”lägsta behörighet" (least privilege) och ”nödvändig åtkomst” (need to know), vilket innebär att varje roll och användare endast ska ha tillgång till den minimala mängd uppgifter som krävs för att utföra de aktiviteter som de har tilldelats. Varje roll som har ett legitimt skäl att få tillgång till och hantera information på uppdrag av Svenska kyrkan ska ges minsta möjliga nivå av åtkomst till information för att kunna utföra sina arbetsuppgifter. Riktlinjerna för styrning av åtkomst ska dokumenteras tillräckligt detaljerat och noggrant för att anses vara i linje med bästa praxis. Leverantören ska införa lämpliga kontroller och begränsningar för åtkomst till information och tillträde till lokaler där Svenska kyrkans information hanteras. Uppdelning av arbetsuppgifter och motsvarande åtkomsträttigheter ska formellt dokumenteras med tydliga regler i syfte att säkerställa att kritiska verksamhetsprocesser inte är beroende av en enda person. Roller med privilegierade åtkomsträttigheter ska dokumenteras och endast tilldelas ett minsta antal betrodda personer med relevanta arbetsuppgifter.	

4. Ändrings-hantering	Ändringar av informationsresurser ska hanteras och genomföras i enlighet med en formell process för ändringshantering. Testning av ändringar ska utföras i separata miljöer som inte är anslutna till produktionsmiljöer som används för hantering av känslig information. Fiktiva data ska användas i den mån det är möjligt vid utförandet av tester och kompensatoriska kontroller ska användas om det inte är möjligt att använda fiktiva data.	
5. Hantering av leverantörsrelationer	Hantering och behandling av Svenska kyrkans information får endast utföras av underleverantörer som formellt godkänts av Svenska kyrkan. Underleverantörer till Leverantören ska tillhandahålla garantier för att tillräckliga och lämpliga organisatoriska och tekniska kontroller tillämpas. Leverantören ska säkerställa att känslig information kan skyddas tillräckligt innan ett samarbete inleds. Leverantören ska fortlöpande genomföra formella granskningar av underleverantörernas uppfyllnad av de krav som fastställs i denna säkerhetsbilaga. Om Leverantören anlitar en underleverantör för behandling och hantering av Svenska kyrkans information måste Svenska kyrkan underrättas innan outsourcing påbörjas. Om Leverantören anlitar en underleverantör för behandling och hantering av Svenska kyrkans information ska alla krav i denna säkerhetsbilaga förmedlas i sin helhet och ingå i formella avtal mellan Leverantören och dess underleverantörer. Anställda hos Leverantören eller någon av dess underleverantörer som hanterar Svenska kyrkans information ska omfattas av detaljerade och specifika sekretessavtal i linje med denna säkerhetsbilaga.	
6. Hantering av informationssäkerhets incidenter	Om en informationssäkerhetsincident inträffar hos Leverantören eller någon av dennes underleverantörers organisationer eller anläggningar ska Svenska kyrkan omedelbart och utan dröjsmål informeras. Om incidenter avser personuppgifter som omfattas av EU:s dataskyddsförordning, ska rapportering ske senast 24 timmar efter det att incidenten upptäckts.Leverantören ska skyndsamt genomföra en bedömning avseende om incidenten kan leda till obehörigt avslöjande, förstörelse eller manipulering av Svenska kyrkans information. Leverantören ska formellt rapportera resultaten av bedömningen till Svenska kyrkan. Leverantören ska ha en plan med detaljerade instruktioner för effektiv och samordnad hantering av säkerhetsincidenter. Leverantörens plan ska vara formellt dokumenterad och innehålla en förteckning över åtgärder för att åtgärda incidenter, inklusive uppgifter avseende relevant personal för vanligt förekommande incidenter. Planen ska kommuniceras till samtliga relevanta parter inom och utanför Leverantörens organisation.	

	Upptäckten av informationssäkerhetsincidenter ska skyndsamt meddelas till Informationssäkerhetssamordnare på Svenska kyrkan. Leverantören ska inte kontakta myndigheter på Svenska kyrkans vägnar, men förväntas bistå Svenska kyrkan vid händelse av en säkerhetsincident. Säkerhetsrelaterade incidenter ska dokumenteras. Denna ska innehålla uppgifter gällande omständigheter som ledde fram till incidenten, loggar för incidenthantering, analys avseende grundorsaken och åtgärder för att undvika liknande incidenter i framtiden.	
7. Informationssäkerhetsaspekter avseende planering av kontinuitet	Leverantörens kontinuitetsplan för verksamheten är avgörande för att samordna nödvändiga åtgärder i händelse av oförutsägbara tjänsteavbrott. Leverantören ska ha rutiner för att säkerställa överenskomna nivåer av kontinuitet och tillgänglighet för alla it-system och manuella processer som hanterar Svenska kyrkans information. Leverantörens kontinuitetsplan ska vara formellt dokumenterade och tillräckligt detaljerade i enlighet med bästa praxis. Kontinuitetsplanen ska innehålla detaljerade återställningsrutiner och it-lösningar för vanligt förekommande situationer som resulterar i tjänsteavbrott, inklusive formellt fastställda roller och ansvarsområden för Leverantörens personal.	
8. Personalsäkerhet	Leverantören ska säkerställa att all personal, såväl anställda som kontrakterad extern personal samt underleverantörer, får adekvat information avseende säkerhetsansvar och säkerhetskontroller i samband med personalens arbetsuppgifter och tillämpbara krav som följer av denna säkerhetsbilaga samt alla tillämpbara externa krav, så som verksamhetskrav och lagstadgade krav. Leverantören ska tillhandahålla säkerhetsutbildning för all nyanställd personal som är anpassad till deras specifika ansvarsområden och arbetsuppgifter som är relevant för tjänsten eller produkten. Leverantören ska tillhandahålla säkerhetsutbildningsprogram som är anpassade till särskilda målgrupper som arbetar med känslig information och/eller arbetsuppgifter med hög informationsrisk, så som HR, tekniker, kundtjänst, it-personal osv. Leverantören ska ha ett årligt utbildningsprogram med definierade kunskapsmål och framgångskriterier för personal som hanterar känslig information.	
9. Hantering av känslig information	För att säkerställa att skyddsvärd information från Svenska kyrkan inte röjs ska Leverantören säkerställa att all personal som hanterar Svenska kyrkans informationstillgångar uppvisar tillräckliga sekretessgarantier, både i form av formella sekretessavtal och tillräcklig expertis och integritet. För att uppnå detta syfte ska särskilda åtgärder vidtas för att säkerställa att personal som är involverad i hanteringen eller behandlingen av information från Svenska kyrkan informeras om sina skyldigheter gällande hantering av känslig information, samt för att säkerställa att Leverantörens egna krav på sina anställda föreskriver tillräckliga tillämpliga förväntningar gällande hantering av känslig information.	

Tekniska säkerhetsåtgärder

	Säkerhetsåtgärd	**Leverantören säkerställer åtgärden genom – ange svar nedan**
10. Autentisering	Standardautentisering - dvs. varje användare ska ha ett unikt användar-ID i kombination med ett starkt lösenord. Lösenordskomplexiteten ska upprätthållas, lösenord ska ändras regelbundet och kontot ska låsas efter ett fördefinierat antal felaktiga lösenord. Behovet av strängare autentiseringsrutiner, dvs. tvåfaktorsautentisering, ska beslutas utifrån risk (t.ex. all extern åtkomst från Internet eller tjänster som ofta är måltavlor för intrångsförsök).	
	Autentiseringsuppgifter krypteras och/eller hashas med ett salt när de lagras. Användarnamn och autentiseringsuppgifter för konton överförs över nätverk med hjälp av krypterade kanaler. Tvåfaktorsautentisering för administratörskonton	
11. Styrning av åtkomst	Begäran om åtkomst till system följer reglerna för uppdelning av arbetsuppgifter Behörigheter för åtkomst till system är rollbaserade och följer principen om lägsta behörighet Delade konton är inte tillåtna om det inte finns rutiner för att identifiera enskilda användares aktiviteter. Automatiserad process för att återkalla åtkomst till system genom att inaktivera konton omedelbart när en anställd eller en uppdragstagare slutar eller byter ansvarsområde.	
12. Tilldelning av roller och grupper	Övervaka tilldelningen av privilegierade grupper och roller för att förhindra obehörig utökning av privilegier, och regelbundet se över medlemskapet i dessa grupper och roller för att bekräfta behovet av privilegierad åtkomst. Säkerställa att användare tilldelas roller och grupper i enlighet med principen om lägsta behörighet	
13. Lagring och kommunikation	Kryptering på transportlagret, dvs. när nätverkstrafik eller data överförs mellan klienter (webbläsare) och webbapplikationsservern eller back-end och andra komponenter som inte är webbläsare.	
14. Loggar	Möjliggöra systemloggning på alla system som hanterar information från Svenska kyrkan. Möjliggöra att systemloggning inkluderar detaljerad information gällande ”event source”, datum, användare, tidsstämpel, ”source addresses”, ”destination addresses”, och andra relevanta parametrar.	
	Loggning och granskning av administratörsbehörigheter	

15. Skydd mot skadlig kod	Använda centralt hanterad programvara för skydd mot skadlig kod för att kontinuerligt övervaka och skydda organisationens samtliga datorer och servrar.	
16. Sårbarheter	Regelbunden teknisk sårbarhetsbedömning, inklusive åtgärder för att minska sårbarheten i externa system och servrar.	
17. Change Management	Ändringsprocess ska finns på plats, endast godkända ändringar får genomföras.	
18. Hantering av patchar	Process för hantering av patchar, ska finnas på plats, inklusive rutin för kritiska säkerhetspatchar.	
19. Nätverk	Brandväggar och ”local end-point protection” övervakas aktivt för att observera avvikelser i trafik och intrång. It-system som hanterar Svenska kyrkans information bör placeras i separata nätverkssegment som hålls åtskilda från klient-, gäst- och nätverkssegment som används i testsyfte.	
20. Fjärråtkomst	Övervaka fjärråtkomstanslutningar för att säkerställa att de överensstämmer med organisationens krav för säker åtkomst.	
21. Återställning av data	Det ska finnas möjlighet att säkerhetskopiera information från Svenska kyrkan på lokal lagringsmedia.	
22. Applikationsutveckling och säkerhet	Fastställa säkra kodningsmetoder, t.ex. OWASP SAMM, som är lämpliga för det programmeringsspråk och den utvecklingsmiljö som används. Verifiera att versionen av all programvara som införskaffats utanför din organisation fortfarande stöds av utvecklaren alternativt att den är tillräckligt skyddad enligt utvecklarens säkerhetsrekommendationer. Endast använda uppdaterade och pålitliga tredje part komponenter för programvaran som utvecklats av organisationen. Se till att all personal som arbetar med applikationsutveckling får utbildning i att skriva säker kod för sin specifika utvecklingsmiljö och sitt ansvarsområde. Upprätthålla separata miljöer för produktionssystem och icke-produktionssystem. Utvecklare bör inte ha oövervakad tillgång till produktionsmiljöer. Skydda webbapplikationer genom att driftsätta brandväggar för webbapplikationer (WAF) som granskar all trafik som strömmar till webbapplikationen för att upptäcka vanliga attacker mot webbapplikationer. För applikationer om är beroende av en databas ska ”standard hardening configuration templates” användas. Alla system som ingår i kritiska affärsprocesser bör också testas.	
23. Fysisk säkerhet	Tillgång till anläggningar och byggnader där Svenska kyrkans information lagras och/eller	

	hanteras får endast ges till behörig personal. Itresurser och utrustning som hanterar Svenska kyrkans information bör skyddas i anläggningar med bemannad reception eller elektroniska system för åtkomstkontroll (passerkort och koder) som kontrollerar det fysiska tillträdet till byggnaden. Brandskydd så som brandlarm och anpassad brandsläckningsutrustning, ska finnas i alla lokaler där Svenska kyrkans information hanteras. Brännbart material får inte förvaras i säkra utrymmen. Ändamålsenliga miljökontroller så som kylning ska kompensera för det värmeöverskott som It-utrustningen genererar. It-utrustning som hanterar Svenska kyrkans information bör också skyddas mot miljörisker som fukt och statisk elektricitet.	