الزامات امنیتی قرارداد

منظور از الزامات امنیتی رعایت اصول محرمانگی، صحت و دسترس‌پذیری داده‌ها، اطلاعات و منابع سازمان است. در این راستا، ضروری است فروشنده (مجری) پارامترهای امنیتی ذیل را در تمامی چرخه عمر سیستم (تولید، توسعه و پشتیبانی) در نظر گرفته و به‌طور مستمر مورد بازبینی و نظارت قرار دهد. در ادامه فعالیت‌های لازم جهت نیل به این هدف ارائه شده است.

۱ .پورت‌های ارتباطی سرور مطابق با سیاست‌ها و پروتکل‌های امنیتی فاوا و با تأیید راهبر سامانه باز خواهد شد و دسترسی عمومی آن محدود می‌باشد. ایجاد دسترسی از راه دور برای پیمانکار از طریق VPN، اعلام IP ثابت و پورت مشخص و تنها در زمان‌های محدود امکان‌پذیر است.

۲ .دسترسی سرورها به اینترنت تنها با درخواست پیمانکار و تایید درخواست توسط راهبر سامانه در سمت کارفرما برای مدت زمان محدود امکان‌پذیر است.

۳ .پیمانکار متعهد می‌گردد پیش از اعمال هرگونه تغییر در طراحی و پیاده‌سازی نرم افزار یا مدیریت کاربران و سطوح دسترسی، تاییدیه راهبر سامانه در سمت کارفرما را دریافت نماید.

۴ .پیمانکار متعهد می‌گردد در صورت نیاز به چندین دسترسی مدیریتی در سطح سامانه و پایگاه داده برای هر یک از افراد، حساب کاربری مجزا و اختصاصی ایجاد شود.

۵ .پیمانکار متعهد می‌گردد که رمزهای عبور در هیچ قسمتی از سامانه یا پایگاه داده به صورت Plaintext (بدون رمزنگاری) ذخیره نشود. همچنین در صورت نیاز به استفاده از رمز عبور محلی، سامانه نباید اجازه دهد که رمزهای عبور بدون رعایت الزامات طول و پیچیدگی مناسب تنظیم شود.

۶ .پیمانکار متعهد می‌گردد که در صورت امکان فنی، اقدامات لازم در خصوص جداسازی سرورهای برنامه کاربردی و پایگاه داده را با هماهنگی کارفرما اتخاذ نماید.

۷ .پیمانکار موظف است کلیه اقدامات لازم به منظور همکاری در نصب آخرین وصله‌های امنیتی (Patch) در سطح سامانه و پایگاه داده را بلافاصله بعد از انتشار و تأیید پایداری آن‌ها به عمل آورده و اقدامات لازم برای سازگاری سامانه با این وصله‌ها را انجام دهد.

۸ .پیمانکار متعهد است در صورت مشاهده رخداد امنیتی مرتبط با سامانه، شواهد را به مسئول امنیت کارفرما ارائه و نسبت به امن‌سازی سامانه در قالب یک درخواست اضطراری، اقدام فوری نماید. همچنین در صورت اعلام کارفرما مبنی بر رخداد امنیتی بر روی سامانه، پیمانکار بایستی نسبت به بررسی لاگ‌های امنیتی و رفع مشکل در قالب موارد اضطراری، اقدام فوری انجام دهد. ذخیره‌سازی و نگهداری لاگ‌های امنیتی بایستی به نحو مقتضی و با نظر کارشناس امنیت کارفرما انجام پذیرد.

۹ .تبادل اطلاعات حوزه قرارداد از طریق پست‌های الکترونیکی عمومی از قبیل یاهو، جیمیل و غیره ممنوع می‌باشد و در این راستا ضروری است ارسال اطلاعات از طریق پست الکترونیکی دامنه شرکت و یا نهایتاً هاست‌های داخل کشور صورت گیرد و مقصد ارسال نیز باید پست دانشگاهی راهبر سامانه، مسئول امنیت و یا سایر کارشناسان/مسئولین ذیربط باشد.