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.

واژگان کاربردی:

- خریدار: دانشگاه اصفهان
- راهبر سامانه: مسئول مدیریت و راهبری سامانه سمت خریدار
- مسئول امنیت: مسئول امنیت شبکه و سامانه‌های اطلاعاتی سمت خریدار
- مسئول اداری/ مالی: مسئول امور اداری، مالی و قراردادهای خریدار

سیاست‌های امنیتی در حوزه نگهداری و مانیتورینگ سرور، پایگاه داده و برنامه کاربردی
۱. عدم استفاده از سرورها جهت امور غیر از کارکرد اصلی سامانه
۲. عدم اشتراک‌گذاری فایل‌ها، دسترسی‌ها و اطلاعات بر روی سرور بدون کسب مجوز
۳. کنترل سرویس‌های فعال و غیرفعال کردن سرویس‌های غیرضروری متناسب با سامانه‌ی موضوع قرارداد بر روی سرورهای تحت پوشش سامانه (نظیر File & Printer Sharing، Telnet و غیره)
۴. همکاری در انجام فعالیت‌های مقاوم‌سازی (Hardening) سرورهای تحت پوشش سامانه در مواردی که این مقاوم‌سازی با عملکرد سامانه ارتباط پیدا می‌کند.
۵. پرهیز از نصب نرم‌افزارهای غیرضروری بر روی سرورهای تحت پوشش سامانه (از جمله برنامه‌های مدیریت سرور و سرویس‌دهنده از راه‌دور). در این راستا ضروری است لیست تأیید شده نرم‌افزارهای نصب شده روی سرور به راهبر سامانه تحویل داده شود.
۶. جداسازی سرورهای برنامه کاربردی و پایگاه داده در صورت وجود امکان فنی
۷. همکاری در فعال‌سازی آنتی‌ویروس مورد تأیید خریدار بر روی سرورهای تحت پوشش سامانه
۸. استفاده از پروتکل ارتباطی HTTPS برای برنامه‌های کاربردی تحت وب با همکاری خریدار
۹. محدودسازی پورت‌های باز سرور متناسب با نیاز سامانه، مسدودسازی پورت‌های غیرضروری و تغییر پورت پیش‌فرض سرویس‌ها. لازم به ذکر است پورت‌های دسترسی برای راهبری سامانه با سیاست‌ها و پروتکل‌های امنیتی خاص مورد تأیید خریدار نظیر محدودسازی IP یا نظایر آن و با تأیید راهبر سامانه باز خواهد شد و دسترسی عمومی آن محدود می‌باشد (ایجاد دسترسی از راه دور برای مجری از طریق VPN و اعلام IP ثابت و پورت مشخص و تنها در زمان‌های محدود امکان‌پذیر است).
۱۰. دسترسی سرورها به اینترنت تنها با درخواست فروشنده و تایید درخواست توسط راهبر سامانه برای مدت زمان محدود امکان‌پذیر است.
۱۱. مدیریت دسترسی کاربران (کنترل دسترسی سرور، بانک اطلاعاتی و برنامه کاربردی) شامل:
a. فروشنده موظف است کاربران مدیریتی پیش فرض (مانند Administrator یا Root) را غیرفعال و جایگزین نماید و رمز عبور مدیر سیستم (Server Admin)، مدیر پایگاه داده (Database Admin) و مدیر سامانه (Application Admin) را حداقل به‌صورت فصلی تغییر و در قالب یک نامه محرمانه (در پاکت در بسته) در اختیار ریاست مرکز فناوری اطلاعات قرار دهد. تغییر سطوح دسترسی کاربران مدیریتی بایستی با تأیید نماینده خریدار باشد.
b. در صورت نیاز به چندین دسترسی مدیریتی بایستی برای هر یک از افراد، حساب کاربری مجزا و اختصاصی ایجاد شود.
c. امکان تعریف نام‌های کاربری منحصر به فرد با سطوح دسترسی کنترل شده برای کلیه کاربران
d. غیرفعال‌سازی دسترسی‌های غیر کاربردی و پیش فرض

e. اعمال محدودیت زمانی برای کاربران
f. ثبت لاگ فعالیت کاربران بر روی کارکردهای اصلی سامانه

تبصره ۱: در صورتی‌که فروشنده برای انجام تعهدات موضوع این قرارداد، نیازی به رمزهای عبور مدیریتی نداشته باشد، ضروری است که این موضوع را به‌صورت مکتوب به خریدار اعلام نماید. بدیهی است که کلیه مسئولیت‌های ناشی از عدم دسترسی فروشنده به رمزهای عبور بر عهده فروشنده خواهد بود.

۱۲. پیاده‌سازی کنترل‌های امنیتی در قسمت ورود به برنامه کاربردی شامل محدودسازی تعداد دفعات تلاش برای ورود، CAPTCHA و کنترل تزریق ورودی غیر مجاز

۱۳. 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.

۱۴. رمزهای عبور نباید به صورت Plaintext (بدون رمزنگاری) در هیچ قسمتی از سامانه ذخیره شود.

۱۵. پس از استقرار سامانه در محل خریدار و پیش از تحویل نهایی، ارزیابی و پویش آسیب پذیری‌های حوزه وب، سیستم عامل، پایگاه داده و ارتباطات شبکه و اجرای آزمایش‌های نفوذ جعبه سفید و جعبه سیاه توسط فروشنده الزامی است و بایستی گزارشات مربوطه به خریدار ارائه گردد.

۱۶. فروشنده موظف است کلیه اقدامات لازم به منظور نصب و یا همکاری در نصب آخرین وصله‌های امنیتی (Patch) سیستم عامل، پایگاه داده و سایر اجزای سامانه موضوع قرارداد را بلافاصله بعد از انتشار و تأیید پایداری آن‌ها به عمل آورده و اقدامات لازم برای سازگاری سامانه با این وصله‌ها را انجام دهد. بایستی فروشنده حداقل به‌صورت فصلی گزارشی مبنی بر رصد حفره‌های امنیتی پایگاه داده، وب سرور و برنامه کاربردی و اقدامات انجام شده در راستای نسخه‌های به‌روزرسانی و نصب شده ارائه دهد.

سیاست‌های امنیتی در حوزه پاسخ گویی به رویدادهای امنیتی

۱. فروشنده متعهد است در صورت مشاهده رخداد امنیتی مرتبط با موضوع قرارداد، شواهد را به مسئول امنیت خریدار ارائه و نسبت به امن‌سازی سامانه در قالب یک درخواست اضطراری، اقدام فوری نماید.

۲. فروشنده متعهد است در صورت اعلام خریدار مبنی بر رخداد امنیتی بر روی سامانه، نسبت به بررسی لاگ‌های امنیتی و رفع مشکل در قالب موارد اضطراری، اقدام فوری انجام دهد.

سیاست‌های امنیتی در حوزه تبادل اطلاعات

۱. امضای تعهدنامه عدم افشای اطلاعات و ارائه آن به مسئول امور اداری/مالی خریدار

۲. عدم ارسال اطلاعات از طریق پست‌های الکترونیکی عمومی از قبیل یاهو، جیمیل و غیره. 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.