



الزامات فنی ارائه‌ی سامانه‌های نرم افزاری توسط تأمین‌کنندگان

گروه تحقیق و توسعه – مرکز توسعه فناوری اطلاعات، امنیت و هوشمند سازی



فهرست مطالب

۱		واژگان کاربردی
۱		مقدمه
۱		الزامات عمومی
۱		مستند سازی و تحلیل نیازمندی‌ها
۲		الزامات فنی و مسئولیت‌های پیمانکار
۲		الزامات معماری
۲		الزامات پایگاه داده
۲		الزامات رابط کاربری (Front-end)
۳		الزامات هسته‌ی سامانه (Back-end)
۳		الزامات استقرار (Deployment)
۳		الزامات نگهداری و پشتیبانی
۳		الزامات قانونی
۴		الزامات امنیتی



واژگان کاربردی

- فاوا: مرکز توسعه فناوری اطلاعات، امنیت و هوشمند سازی
- نماینده‌ی دانشگاه: مسئول (ین) مربوطه در مرکز فاوا دانشگاه اصفهان
- تأمین کنندگان - پیمانکار: شرکت‌های ارائه دهنده‌ی سامانه‌های نرم افزاری
- بهره بردار: معاونت و یا بخشی از سازمان که بهره‌بردار نهایی از سامانه می‌باشد.
- افتا: مرکز امنیت فضای تولید و تبادل اطلاعات
- ماهر: مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای

مقدمه

شرکت‌های متقاضی همکاری در طراحی، توسعه یا فروش نرم‌افزارهای دانشگاهی ملزم به رعایت دقیق الزامات فنی ذیل می‌باشند. این استانداردها با هدف تضمین کیفیت، امنیت و پایداری سامانه‌ها تدوین شده و مبنای ارزیابی فنی پیشنهادات شما خواهد بود. تعیین این الزامات باعث مشخص شدن چارچوبی شفاف برای تحویل پروژه مطابق استانداردهای روز، کاهش ریسک هزینه‌های اضافی ناشی از بازبینی و اصلاحات و ایجاد رقابتی عادلانه بین پیمانکاران بر اساس معیارهای یکسان می‌باشد. همچنین رعایت این الزامات باعث تسهیل در فرآیند تحویل و پذیرش نهایی پروژه و کاهش احتمال نیاز به بازبینی‌های مکرر و هزینه‌بر سامانه‌های نرم‌افزاری خواهد شد.

الزامات عمومی

مستند سازی و تحلیل نیازمندی‌ها

- برگزاری جلسات کارشناسی پیمانکار با نمایندگان دانشگاه (از جمله بهره بردار سامانه و کارشناسان مرکز توسعه فناوری اطلاعات، امنیت و هوشمند سازی - فاوا) قبل از عقد قرارداد و یا توسعه‌ی نرم افزار.
- پس از برگزاری جلسات مشترک، پیمانکار موظف است پیش از عقد قرارداد و با هماهنگی نمایندگان دانشگاه، سند «شرح نیازمندی‌های اولیه پروژه» را ارائه نماید که شامل اهداف کلی، قابلیت‌های اصلی و محدودیت‌های کلیدی از جمله الزامات مقیاس‌پذیری (مانند تعداد کاربران همزمان و حجم داده) و زمانی (مهلت‌های تحویل هر فاز) می‌باشد. مستندات باید به زبان فارسی و با پشتیبانی از اصطلاحات فنی انگلیسی تهیه شوند.



الزامات فنی و مسئولیت‌های پیمانکار

- پیمانکار باید تسلط کامل به سیستم عامل و زبان برنامه‌نویسی نرم افزار ارائه شده و دانش فنی اولیه در خصوص نرم افزارهای لینوکس و پایگاه داده را داشته باشد. دانشگاه هیچ مسئولیتی در راهنمایی فنی، راه‌اندازی محیط‌ها یا رفع مشکلات فنی ندارد.
- پیمانکار موظف است تمام مراحل توسعه، تست و راه‌اندازی نهایی را به صورت مستقل انجام دهد و محیط عملیاتی را آماده کند.

الزامات معماری

- جداسازی لایه‌های واسط کاربری (Presentation) و هسته‌ی سامانه (Business Logic) و پایگاه داده (Data Access) در صورت امکان فنی، جهت افزایش قابلیت نگهداری، مقیاس پذیری و امنیت نرم افزار.
- استفاده از Microservices در صورتی که سامانه در شرایط خاصی نیازمند مقیاس‌پذیری بالا و تحمل ترافیک بالا می باشد.

الزامات پایگاه داده

- طراحی نمودار موجودیت-رابطه (EDR) و Schema در نرم افزار Microsoft Visio یا Lucidchart و ارائه مستندات طراحی به مرکز فاوا دانشگاه و دریافت تاییدیه قبل از پیاده‌سازی.
- از InnoDB به عنوان موتور ذخیره‌سازی در پیکربندی MySQL استفاده شود. در موارد خاصی که نیاز باشد نوع دیگری در نظر گرفته شود، با ذکر دلایل، تاییدیه مرکز فاوا گرفته شود.
- تنظیم Indexing برای جداول پرکاربرد با جست و جوی بالا در سامانه.
- پشتیبان‌گیری از اطلاعات به صورت اتوماتیک و امکان پشتیبان‌گیری دستی و اختیاری در زمان دلخواه.

الزامات رابط کاربری (Front-end)

- سامانه واکنش‌گرا (Responsive) باشد و در نمایش با تمامی دستگاه‌ها (از موبایل تا دسکتاپ) سازگاری داشته باشد.
- با هماهنگی مرکز فاوا، از رنگ‌ها، لوگو و تصاویر دانشگاه اصفهان در رابط کاربری استفاده شود.
- تطابق سامانه با مجموعه استاندارد‌های بین‌المللی WCAG، حداقل سطح AA، جهت برقراری دسترسی پذیری به کلیه‌ی کاربران سامانه. به طور مثال، پشتیبانی از صفحه‌خوان (Screen Reader) مانند NVDA در صفحات ترجیحاً استفاده از تکنولوژی‌های جدید مانند React.js یا Vue.js در پیاده‌سازی رابط کاربری.



الزامات هسته‌ی سامانه (Back-end)

- مستند سازی بر روی متن کد انجام شود.
- امکان تبادل اطلاعات بین سامانه‌ی ارائه شده و سایر سامانه‌های دانشگاه اصفهان، بنا به تشخیص مرکز فاوا (بر اساس استاندارد تعیین شده، از طریق ارائه‌ی وب‌سرویس و یا پیاده‌سازی API در سطح برنامه) وجود داشته باشد.
- اجرای فرآیند Unit Test و Integration Test در سامانه‌هایی که دارای منطق پردازشی پیچیده هستند.
- استفاده از سرور Apache یا Nginx و یا سرویس IIS در صورت نیاز و هماهنگی نماینده‌ی دانشگاه.

الزامات استقرار (Deployment)

- توسعه در محیط پیاده‌سازی شخصی پیمانکار انجام شده و تست سامانه در محیط ایزوله دانشگاه با داده‌های آزمایشی انجام می‌پذیرد. پیمانکار مسئول تولید داده‌های تستی مورد نیاز است. در موارد استثنایی و صرفاً با تأیید کارفرما، ممکن است داده‌های واقعی جهت تست ارائه شود که در اینصورت این داده‌ها مشمول تعهدنامه عدم افشای اطلاعات می‌باشد. در نهایت، سامانه در فاز عملیاتی روی سرور اختصاصی دانشگاه استقرار می‌یابد. مسئولیت استقرار کامل سامانه روی سرور اصلی دانشگاهی به عهده‌ی پیمانکار می‌باشد.
- ارائه نسخه آزمایشی (Beta) برای بازبینی دانشگاه قبل از تحویل نهایی.

الزامات نگهداری و پشتیبانی

- ارائه برنامه نگهداری سالانه به مرکز فاوا.
- پیمانکار ملزم به ارائه گزارش ماهانه پیشرفت به مرکز فاواست و در صورت اختلاف فاحش با زمانبندی قرارداد، طبق شرایط قرارداد، به منظور حفظ حقوق دانشگاه، عمل خواهد شد.
- به‌روزرسانی مستمر امنیتی و عملکردی سامانه با هماهنگی نماینده‌ی دانشگاه.
- در صورت نیاز، برگزاری کارگاه‌های آموزشی برای بهره‌برداران نهایی سامانه.

الزامات قانونی

- پیمانکار موظف است سامانه را مطابق آخرین استانداردهای امنیتی پیاده‌سازی و گواهی معتبر از مراجع ذیصلاح (افتا/ماهر) دریافت نماید. کلیه هزینه‌های مرتبط منحصراً برعهده پیمانکار بوده و کارفرما هیچ تعهدی در این خصوص ندارد.
- مالکیت کد منبع و مستندات فنی پس از تحویل، طبق قرارداد تعیین می‌گردد.



- رعایت قوانین کپی‌رایت و عدم استفاده از کتابخانه‌های دارای محدودیت تجاری.

الزامات امنیتی

- قابلیت یکپارچه‌سازی با سامانه احراز هویت مرکزی (SSO) دانشگاه اصفهان.
- پشتیبانی از رمزعبور پیچیده و در صورت نیاز احراز دو مرحله‌ای (2FA) در سامانه‌های دارای حساسیت بالا و جهت جلوگیری از حملات phishing
- عدم ذخیره رمزهای عبور بدون روش رمزنگاری و به صورت Plaintext و رمزنگاری داده‌های حساس با استاندارد AES-256
- بهره‌گیری از روش‌های ایمن در کدنویسی به منظور جلوگیری از حملات احتمالی. به طور مثال استفاده از روش‌های Prepared Statements و یا ORM برای جلوگیری از حملات SQL Injection.
- ثبت تمام فعالیت‌های کاربران در Log Files با ارائه‌ی پلتفرم مورد تایید مرکز فاوا و با قابلیت بررسی توسط این مرکز.
- انجام تنظیمات پروتکل ارتباطی HTTPS در تمامی صفحات با هماهنگی مرکز فاوا.
- پیاده‌سازی کنترل‌های امنیتی در قسمت ورود به برنامه کاربردی شامل محدودسازی تعداد دفعات تلاش برای ورود، CAPTCHA و کنترل تزریق ورودی غیرمجاز.
- پس از استقرار سامانه در محل خریدار و پیش از تحویل نهایی، ارزیابی و پایش آسیب‌پذیری‌های 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.