معیارهای ارزیابی شرکت متقاضی دریافت پروانه خدمت «**آزمون و ارزیابی امنیتی**»

جدول (۱). جدول معیارهای ارزیابی

معیار	ریزمعیار	توضیحات
فنی	صحت، دقت و کیفیت گزارش انجام پروژه	بررسی گزارش فنی پروژه انجام شده براساس موارد ذیل: • برای انجام آزمون تنها از ابزار استفاده شده یا دستی نیز بررسی شده است؟ (هر چه میزان بررسی دستی بیشتر باشد امتیاز این بند بیشتر خواهد شد) • در گزارش، خروجی ابزار آزمون بیان شده یا اینکه توضیحاتی از زبان کارشناسان ذکر شده است؟ (خروجی ابزار کمترین امتیاز را دارد) • برای یک آسیب‌پذیری، PoC بیان شده است یا خیر؟ (اکسپلویت انجام شده یا خیر) • درجه سختی آسیب‌پذیری • درجه سختی بهره‌برداری (اکسپلویت) از آسیب‌پذیری • آیا منطق (جریان کاری داده) شبکه/سامانه/برنامه تست شده است؟
	توانایی فنی کارشناسان	• مصاحبه فنی • بررسی سابقه کاری • بررسی مدرک تحصیلی
	محصول (سخت‌افزار، نرم‌افزار) و ابزارهای تولیدی در حوزه خدمت مربوطه	تولید ابزار/نرم‌افزار برای انجام آسیب‌پذیری، به نحوی که کارایی بالاتری از ابزارهای رایگان داشته باشد و یا از لحاظ هزینه بسیار مقرون به صرفه‌تر از ابزارهای تجاری خارجی باشد (اما به همان اندازه کارایی داشته باشد)
	تدوین مستندات فنی در رابطه با چگونگی انجام پروژه/ ثبت تجربه‌های مفید در رابطه با حل چالش‌ها/تدوین مستندات آموزشی برای کارشناسان	این مورد فعلا بررسی نمی‌شود
امنیتی	مدیریت اسناد	بررسی طبقه‌بندی اسناد، نحوه ذخیره مستندات محرمانه، مدیریت نسخ و ...
	ساختار شبکه شرکت	بررسی شبکه از لحاظ موارد ذیل: • Vlan بندی • تعریف Zone های مناسب • سیستم‌های امنیتی تعبیه شده (فایروال، آنتی ویروس و ...) • ثبت رخدادهای ممیزی (لاگ) برای شبکه و نگهداری متمرکز آن
	امنیت فیزیکی	بررسی موارد ذیل: • نحوه کنترل ورود و خروج • دوربین مدار بسته • سیستم اعلام و اطفاء حریق • محافظت از دیتاسنتر (نصب دوربین، تهویه و سیستم‌های سرمایشی، نحوه دسترسی و ...)
کیفی	محیط فیزیکی شرکت	بررسی محیط شرکت براساس موارد ذیل: • مناسب بودن فضای کاری • جدا بودن بخش امنیت از سایر بخش‌ها • جداسازی گروه‌های کاری (براساس اتاق یا فضای پارتیشن‌بندی شده)

سابقه انجام پروژه	بررسی موارد ذیل: • انجام پروژه در حوزه‌ای که درخواست گواهی داشته است. • انجام پروژه در حوزه‌های مرتبط با گواهی درخواست شده.	
توانایی حفظ نیرو انسانی	بررسی موارد ذیل: • شرکت به چه میزان در حفظ نیروهای فنی خود موفق عمل کرده است؟ • جدایی نیروهای فنی به چه علت‌هایی بوده است؟	
مدیریت ارتباط با مشتری	حداکثر امتیاز به موردی اعطا می‌شود که سامانه‌ای برای ارتباط با مشتری مهیا شده باشد و درخواست مشتری به طور سیستماتیک به کارشناس مربوطه ارجاع شود. همچنین امکان گزارش‌گیری کامل از سامانه وجود داشته باشد.	
نظامنامه کیفی/ آیین نامه‌ها و دستورالعمل‌ها	بررسی نظام‌نامه کیفی، آیین نامه‌ها و دستورالعمل‌های داخلی، ضوابط استخدام و خاتمه همکاری، ضوابط کاری از قبیل مرخصی، ماموریت، ...	
سابقه دریافت گواهی در حوزه خدمت مذکور	بررسی دفعات تمدید گواهی (صرفا برای خدمتی که درخواست داده است)	

جدول (۲). معیارهای سنجش توانایی فنی کارشناسان برای خدمت «**آزمون و ارزیابی امنیتی**»

معیار	تخصص‌های مورد نیاز	منابع
دانش پایه	✓ احراز هویت ✓ کنترل دسترسی ✓ رمزنگاری ✓ آسیب‌پذیری ✓ کدهای مخرب ✓ توپولوژی‌های امنیتی و امنیت زیرساخت	➢ Security+
دانش مقدماتی تست نفوذ	✓ جمع‌آوری اطلاعات و شناسایی هدف ✓ شناسایی و تحلیل مقدماتی آسیب‌پذیری ✓ شنود و آنالیز ترافیک ✓ کرک پسورد ✓ حملات از کار انداختن سرویس ✓ تکنیک‌ها و ابزارهای نفوذ	➢ CEH ➢ SEC504
دانش تخصصی تست نفوذ (شبکه- نرم‌افزار و وب-برنامه-های موبایل (Android, IOS)	✓ حملات وب (Injection, XSS, …) ✓ حملات پیشرفته وب (وب) ✓ ارزیابی فریم‌ورک‌های وب (وب) ✓ تشخیص WAF و راه‌های دور زدن آن (وب) ✓ اسکن عمیق شبکه (شبکه) ✓ بهربرداری (شبکه) ✓ جمع‌آوری داده‌های شبکه و WiFi و آنالیز آن (شبکه) ✓ حملات شبکه WiFi (شبکه) ✓ تهدیدات دستگاه‌های موبایل (موبایل)	➢ SEC542 (Web) ➢ SEC642 (Web) ➢ SEC560 (Network) ➢ SEC617 (Network) ➢ SEC575 (Mobile App)

	✓ آنالیز برنامه‌های موبایل (موبایل) ✓ مهندسی معکوس برنامه‌های موبایل (موبایل) ✓ تست نفوذ برنامه‌های موبایل (موبایل)	
دانش تحلیل آسیب‌پذیری و اکسپلویت نویسی	✓ مدلسازی تهدید ✓ اسکن عمیق آسیب‌پذیری ✓ اعتبارسنجی آسیب‌پذیری ✓ اکسپلویت ویندوز و لینوکس ✓ روشهای فازینگ ✓ مهندسی معکوس با استفاده از IDA ✓ اکسپلویت‌های یک روزه (One-Day) ✓ اکسپلویت سمت کاربر	➢ SEC660 ➢ SEC760

نکات مهم:

- رزومه فنی نیروها و رزومه شرکت، بروزرسانی گردد.
- در صورت وجود هرگونه ابهام، با شماره تلفن‌های مرکز افتای استان گیلان (**۳۳۲۳٤۷۲۰** و **۳۳۲۳٤۷۳۰**) تماس گرفته شود.