معیارهای ارزیابی شرکت متقاضی دریافت پروانه خدمت «**ممیزی انطباق با استانداردهای امنیت اطلاعات و ارتباطات**»

جدول (۱). جدول معیارهای ارزیابی

معیار	ریزمعیار	توضیحات
فنی	صحت، دقت و کیفیت گزارش انجام پروژه	بررسی گزارش فنی پروژه‌های انجام شده
	توانایی فنی کارشناسان	• مصاحبه فنی • بررسی سابقه کاری • بررسی مدرک تحصیلی
	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	امتیازدهی براساس انجام پروژه در حوزه‌ای که درخواست گواهی داشته است.
	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/ آئین نامه ها 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 «**ممیزی انطباق با استانداردهای امنیت اطلاعات و ارتباطات**»

معیار	تخصص‌های مورد نیاز	منابع
دانش پایه	✓ مفاهیم پایه امنیت ✓ احراز هویت ✓ کنترل دسترسی ✓ رمزنگاری ✓ آسیب‌پذیری	➢ Security+
دانش تخصصی	✓ تسلط ISO/IEC ۲۷۰۰۱ /۱۷۰۲۱/۱۹۰۱۱/۲۷۰۰۸/۲۷۰۰۷/۲۷۰۰۶/۲۷۰۰۳/۲۷۰۰۲ ✓ قابلیت سنجش، پایش و ارزیابی کارآیی یک سیستم مدیریت امنیت اطلاعات بر اساس ISO/IEC۲۷۰۰۱ ✓ مفاهیم پایه، روش ها و متدها و تکنیک های مدیریت مخاطرات امنیت اطلاعات ✓ ارزیابی مخاطرات امنیت اطلاعات ✓ ارزیابی آسیب پذیری دارایی ها ✓ تسلط بر کنترل‌ها	➢ ISO/IEC۲۷۰۰۱ ➢ ISO/IEC۲۷۰۰۲ ➢ ISO/IEC۲۷۰۰۵

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.