۱ .مقدمه و نیازمندی‌های کلان فاز شناخت

اداره کل دامپزشکی استان کرمانشاه در راستای اجرای پروژه امن‌سازی و مقاوم‌سازی زیرساخت شبکه و فناوری اطلاعات، نیازمند انجام یک فاز شناخت جامع، مستند و مبتنی بر رویکردهای سیستم مدیریت امنیت اطلاعات (ISMS) است. این فاز باید شناخت دقیق و قابل اتکا از وضعیت موجود سازمان، زیرساخت فناوری اطلاعات، دارایی‌های اطلاعاتی، فرآیندها، خدمات، ساختارهای مدیریتی و مخاطرات امنیتی ایجاد نماید تا مبنای طراحی، تصمیم‌گیری و اجرای اقدامات امنیتی در مراحل بعدی پروژه قرار گیرد.

پیمانکار موظف است کلیه فعالیت‌های فاز شناخت را مطابق الزامات استانداردهای مدیریت امنیت اطلاعات، اصول مدیریت ریسک و الزامات امنیتی ابلاغی مراجع ذی‌صلاح اجرا و مستندسازی نماید.

نیازمندی الزام‌آور مبتنی بر سند ماهر(Maher_Document_14040411)

در اجرای این فاز، پیمانکار مکلف است کلیه فعالیت‌ها را به‌گونه‌ای انجام دهد که امکان اخذ تأیید رسمی مرکز ماهر مطابق سند «دستورالعمل تدوین، تصویب داخلی و ارسال برنامه عملیاتی امنیت دستگاه‌های غیرزیرساختی» فراهم گردد.

بر اساس جدول (۱) سند مذکور، کارفرما انتظار دارد خروجی فاز شناخت به‌صورت مستند، قابل ارزیابی و قابل ارائه برای مرکز ماهر، تحقق کامل موارد زیر را تضمین نماید:

۱ .اجرای کامل ردیف اول جدول (۱): مدیریت دارایی

این ردیف شامل:

- شناسایی، ارزش‌گذاری و اولویت‌بندی دارایی‌های فناوری اطلاعات دستگاه
- اعلام اطلاعات دارایی‌های فناوری اطلاعات دستگاه به مرکز ماهر
- مدیریت تغییرات دارایی‌های فناوری اطلاعات دستگاه

۲ .اجرای کامل بند اول ردیف دوم جدول (۱): تدوین، ابلاغ و اجرای خط‌مشی امنیت فناوری اطلاعات دستگاه

این بند شامل:

- تدوین خط‌مشی امنیت فناوری اطلاعات دستگاه
- ابلاغ رسمی خط‌مشی به واحدهای مرتبط

- تدوین سند اجرای عملیاتی خط‌مشی در سطح سازمان

پیمانکار موظف است خروجی‌های فاز شناخت را به‌گونه‌ای تهیه کند که این دو بخش از جدول (۱) سند ماهر، به‌صورت کامل، قابل ارزیابی و قابل تأیید باشند.

۲ .شرح خدمات فاز شناخت

۲–۱ .شناخت سازمان و تعیین دامنه پروژه

پیمانکار موظف است ساختار سازمانی، مأموریت‌ها، فرآیندهای اصلی و پشتیبان، خدمات ارائه‌شده، ساختار فناوری اطلاعات و محدوده زیرساخت مورد بررسی را مطالعه و تحلیل نماید.

حداقل اقدامات مورد انتظار:

- بررسی ساختار سازمانی و واحدهای مرتبط
- شناسایی ذی‌نفعان پروژه
- شناسایی مسئولین و مالکان فرآیندها
- بررسی فرآیندهای کسب‌وکار و خدمات فناوری اطلاعات
- تعیین دامنه فیزیکی و منطقی پروژه
- شناسایی ارتباطات داخلی و برون‌سازمانی
- تهیه مستند وضعیت موجود(As-Is)

خروجی‌ها:

- گزارش شناخت سازمان
- فهرست ذی‌نفعان
- فهرست فرآیندها
- سند تعیین دامنه پروژه
- گزارش وضعیت موجود

۲–۲ .شناسایی و مدیریت دارایی‌های اطلاعاتی

پیمانکار موظف است کلیه دارایی‌های مؤثر در ارائه خدمات فناوری اطلاعات را شناسایی، طبقه‌بندی، ارزش‌گذاری و مستندسازی نماید.

دامنه دارایی‌ها شامل:

- تجهیزات مرکز داده
- سرورها
- تجهیزات شبکه و امنیت
- تجهیزات ذخیره‌سازی
- سامانه‌ها و نرم‌افزارها
- پایگاه‌های داده
- اطلاعات و اسناد
- خدمات زیرساختی
- تجهیزات کاربران نهایی
- خطوط ارتباطی
- منابع انسانی
- خدمات برون‌سپاری شده

حداقل اطلاعات مورد نیاز برای هر دارایی:

- نام و نوع دارایی
- مالک دارایی
- محل استقرار

- سطح محرمانگی، صحت و دسترس‌پذیری
- اهمیت دارایی
- وابستگی‌ها

خروجی‌ها:

- شناسنامه دارایی‌ها
- فهرست دارایی‌ها
- ماتریس طبقه‌بندی دارایی‌ها
- گزارش ارزش‌گذاری دارایی‌ها

۲–۳ .شناسایی خدمات و فرآیندها

پیمانکار موظف است خدمات فناوری اطلاعات، سرویس‌های زیرساختی و فرآیندهای مؤثر بر مأموریت‌های سازمان را شناسایی و ارتباط آنها با دارایی‌ها را مستندسازی نماید.

حداقل موارد بررسی:

- خدمات شبکه
- سرویس‌های زیرساختی
- سامانه‌های کاربردی
- خدمات کاربران
- فرآیندهای عملیاتی و پشتیبان

خروجی‌ها:

- فهرست خدمات
- شناسنامه خدمات

- ماتریس ارتباط دارایی‌ها و خدمات

۲–۴ .شناسایی تهدیدها

پیمانکار موظف است تهدیدهای مؤثر بر دارایی‌ها، خدمات و زیرساخت فناوری اطلاعات را شناسایی و مستندسازی نماید.

دامنه تهدیدها:

- انسانی
- فنی
- سایبری
- مدیریتی
- فیزیکی
- محیطی
- ناشی از تأمین‌کنندگان و اشخاص ثالث

خروجی‌ها:

- فهرست تهدیدها
- ماتریس تهدیدها

۲–۵ .شناسایی آسیب‌پذیری‌ها

پیمانکار موظف است وضعیت موجود زیرساخت، تجهیزات، سرویس‌ها، فرآیندها و کنترل‌های امنیتی را بررسی و آسیب‌پذیری‌های موجود را شناسایی نماید.

دامنه بررسی:

- آسیب‌پذیری‌های فنی
- مدیریتی

- فرآیندی
- فیزیکی
- مرتبط با منابع انسانی

خروجی‌ها:

- گزارش آسیب‌پذیری‌ها
- ماتریس آسیب‌پذیری‌ها

۲–۶ .ارزیابی ریسک

پیمانکار موظف است بر اساس دارایی‌ها، تهدیدها و آسیب‌پذیری‌ها، ارزیابی ریسک را انجام دهد.

حداقل موارد مورد نیاز:

- معیارهای ارزیابی ریسک
- تعیین احتمال وقوع
- تعیین میزان اثر
- تعیین سطح ریسک
- اولویت‌بندی ریسک‌ها

خروجی‌ها:

- گزارش ارزیابی ریسک
- ماتریس ریسک
- فهرست ریسک‌های اولویت‌دار

۲–۷ .تدوین برنامه اقدامات اصلاحی و امنیتی

پیمانکار موظف است بر اساس نتایج ارزیابی‌ها، برنامه اقدامات اصلاحی و امنیتی مورد نیاز برای مراحل بعدی پروژه را تدوین نماید.

حداقل موارد:

- اقدامات فوری، کوتاه‌مدت، میان‌مدت و بلندمدت
- اولویت اجرا
- زمان‌بندی پیشنهادی
- برآورد منابع مورد نیاز
- کنترل‌های امنیتی پیشنهادی

خروجی‌ها:

- برنامه اقدامات اصلاحی
- برنامه مدیریت ریسک
- نقشه راه اجرای پروژه امن‌سازی و مقاوم‌سازی

۳ .خروجی‌های نهایی فاز شناخت

پیمانکار موظف است در پایان فاز شناخت، حداقل مستندات زیر را ارائه نماید:

- گزارش شناخت سازمان
- سند تعیین دامنه پروژه
- فهرست ذی‌نفعان
- فهرست فرآیندها و خدمات
- شناسنامه دارایی‌ها
- ماتریس طبقه‌بندی دارایی‌ها

- گزارش تهدیدها
- گزارش آسیب‌پذیری‌ها
- گزارش ارزیابی ریسک
- ماتریس ریسک
- برنامه مدیریت ریسک
- برنامه اقدامات اصلاحی
- نقشه راه امن‌سازی و مقاوم‌سازی
- گزارش وضعیت موجود(As-Is)

۴ .الزامات و شرایط احراز صلاحیت پیمانکار

پیمانکار باید دارای شرایط زیر باشد:

۱. مجوز معتبر از مرکز مدیریت راهبردی افتا در حوزه خدمات امن‌سازی و مقاوم‌سازی زیرساخت‌ها و سامانه‌ها

۲. سابقه موفق اجرای پروژه‌های مشابه در دستگاه‌های اجرایی یا نهادهای عمومی

۳. برخورداری از نیروی انسانی متخصص در حوزه‌های امنیت اطلاعات، امنیت شبکه، مراکز داده، سیستم‌های عامل، مجازی‌سازی و ارزیابی امنیت

۴. معرفی مدیر پروژه با سابقه مرتبط

۵. تعهد به محرمانگی اطلاعات و ارائه تعهدنامه برای اعضای تیم

۶. توانایی ارائه مستندات در قالب فایل قابل ویرایش وPDF

۷. رعایت الزامات و سیاست‌های امنیتی کارفرما و مراجع ذی‌صلاح

۸. عدم استفاده از ابزارها یا تجهیزات فاقد مجوز یا مغایر با ضوابط امنیتی کشور

۹. ارائه برنامه زمان‌بندی و روش اجرای پروژه پیش از آغاز عملیات

۵ .الزامات اجرای پروژه

- اجرای پروژه مطابق دامنه خدمات و برنامه زمان‌بندی مصوب
- هماهنگی کامل با واحد فناوری اطلاعات و نماینده کارفرما
- عدم انجام هرگونه تغییر در زیرساخت عملیاتی بدون مجوز
- رعایت محرمانگی کلیه اطلاعات و داده‌های سازمان
- تحویل مستندات به‌صورت ساختاریافته و قابل به‌روزرسانی
- قابلیت استفاده خروجی‌ها در مراحل بعدی امن‌سازی، مقاوم‌سازی، ممیزی و نگهداری