جمهوری اسلامی ایران
ریاست جمهوری
مرکز مدیریت راهبردی افتا


# الزامات امنیتی ارائه محصولات نرم افزاری سازمانی به زیرساختهای حیاتی

نسخه ۱,۰ آبان ماه ۹۸

عادی


بسم الله الرحمن الرحيم

# مقدمه

امروزه بکارگیری تکنولوژی، ابزارها و سامانه‌های فناوری اطلاعات در سازمان‌ها با رشد روزافزونی روبه‌رو است. استفاده از این ابزارها و سامانه‌ها در سازمان‌ها به شرط رعایت امنیت می‌تواند بسیار اثربخش باشد اما در صورتی که این محصولات دارای ضعف و آسیب‌پذیری امنیتی باشند، به جای اثرگذاری در سازمان‌ها می‌توانند یک تهدید جدی محسوب شده و خسارات جبران‌ناپذیری را به بار آورند. در این مواقع علاوه بر مصرف‌کننده، هر ارائه‌کننده‌ای که این محصولات را به سازمان‌ها ارائه می‌دهد در قبال این خسارات مسئول و پاسخگو خواهد بود. هدف از این سند ارائه الزاماتی در مرحله ارائه و پشتیبانی محصولات نرم‌افزاری سازمانی و با تاکید بر مسئولیت‌های ارائه‌کنندگان آن‌ها است.

## ۱– قلمرو سند

قلمرو این سند الزامات امنیتی مراحل ارائه و پشتیبانی- اعم از عقد قرارداد، نصب، استقرار و پشتیبانی- محصولات نرم‌افزاری مورد استفاده در سازمان‌ها است. این محصولات می‌تواند شامل سیستم‌های اتوماسیون اداری، حقوق و دستمزد، اداری مالی، حضور و غیاب، سیستم‌های مدیریت محتوا و یا پورتال‌های سازمانی باشد.

بدیهی است که رعایت الزامات توسعه امن محصول نقش غیرقابل انکاری در امنیت این محصولات دارند اما پرداختن به آن‌ها خارج از قلمرو این سند است.

## ۲–اصطلاحات

**سازمان‌ها:** تمامی دستگاه‌های اجرایی مشمول ماده ۵ قانون مدیریت خدمات کشوری

**ارائه‌کننده محصول:** شخصیت حقوقی که محصول را به سازمان ارائه می‌دهد و می‌تواند همان تولیدکننده محصول و یا ارائه‌کننده خدمات نصب و پشتیبانی نیز باشد.

**محصول:** محصولات نرم‌افزاری سازمانی

**محصول داخلی:** محصولی است که تولید کننده آن یک شرکت ایرانی باشد.

## ۳- الزامات کلی

۳-۱ ارائه‌کننده محصول داخلی، باید محصولی را به سازمان‌ها ارائه دهد که گواهی ارزیابی امنیتی را از مرکز مدیریت راهبردی افتا مطابق با فرآیند اخذ گواهی ارزیابی امنیتی محصولات اخذ کرده باشد.

۳-۲ ارائه کننده خدمات نصب و پشتیبانی به سازمان‌ها در صورتی که تولیدکننده محصول نباشد باید پروانه ارائه خدمات نصب و پشتیبانی محصولات نرم افزاری را مطابق با فرآیند اخذ پروانه خدمات اخذ کرده باشد.

۳-۳ ارائه‌کننده محصولات داخلی به سازمان‌ها باید حداقل وابستگی به سکوها و ابزارهای خارجی داشته و در صورت نیاز به تامین ابزارهای خارجی و کدباز قادر به ارائه لایسنس‌های معتبر در این زمینه باشد و راهکارهای مناسب برای تضمین تداوم عملکرد صحیح محصول را ارائه نماید.

۳-۴ ارائه‌کننده باید کلیه اطلاعات به‌روز مرتبط با سازمان‌های سازمان خود شامل اطلاعات تماس، آدرس و نسخه محصول مورد استفاده را در یک سیستم بایگانی مطمئن و امن نگهداری و به صورت مستمر بروزرسانی نماید. در این راستا لازم است به سازمانان تذکر داده شود که در صورت تغییر اطلاعات خود، ارائه‌کننده را از این امر مطلع کنند تا کانال ارتباطی با آن‌ها برقرار باقی بماند.

۳-۵ ارائه‌کننده باید اطلاعات تمامی محصولات به فروش رسیده به سازمان‌ها را به گونه‌ای ثبت و نگهداری نماید که از طریق شناسه مشخص قابل ردگیری باشند. علاوه بر این نسبت به ثبت و نگهداری سوابق کشف و رفع آسیب‌پذیری محصول ارائه شده اقدام نماید. این سوابق حداقل می‌بایست شامل نسخه آسیب‌پذیر، نوع آسیب‌پذیری، تاریخ کشف، شرح و تحلیل، قلمرو، ارزیابی ریسک، نحوه اطلاع از آن، راه‌حل رفع، سازمان‌های سازمان تحت تاثیر و اقدامات صورت گرفته برای آن‌ها باشد.

## ۴- الزامات زمان عقد قرارداد

۴-۱ مسئولیت تامین هر یک از بخش‌های مستقل نرم‌افزاری محصول تعیین شود و به طور دقیق در قرارداد ذکر گردد. این اجزا می‌تواند شامل سیستم عامل، وب سرور و برنامه‌های کاربردی شخص

ثالث (مانند فریم ورک‌ها و کتابخانه‌ها) باشد. در صورتی که ارائه‌کننده وظیفه تامین هر یک از بخش‌های مستقل نرم‌افزاری را که محصول بر روی آن اجرا می‌شود بر عهده دارد، باید تامین امنیت آن‌ها را نیز پذیرفته و تضمین کند و فرآیندهای لازم برای این کار از جمله به‌روزرسانی اجزا، وصله کردن آسیب‌پذیری‌ها، مقاوم‌سازی و پشتیبان‌گیری را انجام دهد.

الف) در محصولاتی که در بستر اینترنت و محلی خارج از مالکیت سازمان جایگذاری می‌شوند، لازم است وظیفه تامین زیرساخت میزبانی و نحوه رعایت دستورالعمل میزبانی امن[1]خدمات وب در قرارداد به درستی تعیین شود. برخی از ملاحظات امنیتی در این دستورالعمل عبارتند از: ذخیره‌سازی امن داده‌های حساس، اطمینان از گرفتن نسخه پشتیبان دوره‌ای، بروزرسانی و نصب آخرین وصله‌های امنیتی وب‌سرورها

۴-۲ ارائه کننده محصول باید وصله‌های امنیتی محصول خود را برای تمام سازمان‌ها – مستقل از قرارداد پشتیبانی داشتن آن سازمان- تا مدت چهار سال پس از قرارداد فروش آن محصول به سازمان از طریق کانالهای مشخص شده در قرارداد ارائه دهد.

۴-۳ ارائه‌کننده باید حداقل پارامترهای در دسترس بودن محصول و حداکثر زمان رفع آسیب‌پذیری‌های کشف شده محصول و زمان پاسخگویی و بازیابی در حوادث امنیتی ، متناسب با شدت آن‌ها را تعیین کند و و در تفاهم‌نامه سطح خدمات[2]قرارداد ذکر کرده و طبق آن عمل کند.

۴-۴ ارائه‌کننده باید هنگام ارائه محصول، کانال مناسب، مطمئن و پایدار را برای ارتباط متقابل با سازمان فراهم آورد. این کانال جهت اطلاع‌رسانی و آگاهی‌رسانی به سازمان در خصوص آسیب‌پذیری‌ها و نحوه کاهش اثرات و رفع آنها، مورد استفاده قرار می‌گیرد. ضمنا این امکان را فراهم می‌آورد که در صورتی که سازمان نیز متوجه وجود آسیب‌پذیری در محصول گردید، در سریع‌ترین زمان ممکن بتواند به شرکت اطلاع‌رسانی دقیق نماید.

۴-۵ سطوح دسترسی مختلف، حقوق دسترسی و چگونگی دسترسی (در محل/دسترسی از راه دور)

[1] – این دستورالعمل توسط مرکز افتا منتشر می‌گردد.

[2] Service-Level Agreement (SLA)

هر سطح به محصول در مراحل نصب و راهبری توسط ارائه‌کننده و سازمان توافق شود و به طور دقیق در قرارداد ذکر گردد. سطوح دسترسی می‌تواند شامل دسترسی مدیر راهبر محصول، مدیر سیستم عامل و مدیر محصول و حقوق دسترسی حداقل می‌بایست شامل اضافه کردن کاربران، مشاهده داده‌های محرمانه، دسترسی به لاگ‌های ممیزی محصول و تغییر در پیکربندی باشد.

۴-۶ مسئولیت و نحوه پشتیبان‌گیری در سه سطح داده، سطح برنامه کاربردی و سطح سیستم باید توسط سازمان و ارائه‌کننده توافق شود و به طور دقیق در قرارداد ذکر گردد و مطابق با آن عمل گردد.

۴-۷ ارائه کننده باید آموزش‌های لازم برای بهره‌برداری از تمام قابلیت‌های محصول را به کارشناسان بهره بردار محصول در سازمان ارائه نماید.

## ۵- الزامات استقرار و راه اندازی محصول

۵-۱ ارائه‌کننده محصول باید در زمان نصب، نام‌های کاربری و کلمات عبور پیش‌فرض تمامی سرویس‌های مرتبط با محصول از جمله پایگاه داده را تغییر داده و نحوه تغییر مجدد آن‌ها را نیز در اختیار سازمان قرار دهد.

۵-۲ ارائه‌کننده باید حداقل الزامات امنیتی مربوط به رمزهای عبور محصول (از قبیل رعایت طول و پیچیدگی مناسب) را طبق سیاست سازمان اعمال نماید.

۵-۳ ارائه‌کننده باید در هنگام استقرار محصول، در صورت تامین زیرساخت توسط سازمان، محیط عملیاتی و محیط تست سازمان را از یکدیگر مجزا کند و بروز رسانی‌ها را ابتدا بر روی محصول مستقر در محیط تستی انجام دهد و پس از اطمینان بر روی محصول مستقر در محیط عملیاتی اعمال نماید.

۵-۴ ارائه‌کننده هنگام نصب محصول باید در تمامی اجزای مستقل بکار رفته در محصول مانند وب‌سرورها از آخرین نسخه‌های پایدار و منطبق با محصول خود استفاده کرده و آخرین وصله‌های امنیتی منتشر شده برای آن‌ها را نصب کند.

۵-۵ ارائه‌کننده محصول باید در زمان ارائه محصول، کلیه مستندات مورد نیاز از جمله معماری استقرار محصول (نحوه قرار گرفتن محصول در محیط عملیاتی) و اطلاعات دیگر شامل پلتفرم‌ها،

تکنولوژی‌ها و وابستگی‌های محصول به نرم‌افزارها، کتابخانه‌های شخص ثالث مورد استفاده در محصول، سرویس‌های اجرایی، پورت‌ها و دسترسی فایل‌ها به هر پورت را جهت راهبری محصول را جهت راهبری محصول در اختیار سازمان قرار دهد.

۵-۶ ارائه‌کننده در محصولات تحت وب باید تضمین نماید که برای جلوگیری از افشای اطلاعات حساس، نمایش جزئیات خطاهای برنامه و اطلاعات نسخه که ممکن است به صورت پیش‌فرض در صفحات وب (مانند banner،footer و header) موجود باشد غیرفعال و یا حذف شود.

۵-۷ ارائه‌کننده محصول باید پلاگین‌ها و قابلیت‌های کارکردی محصول و زیرساخت‌های مرتبط به آن را که خارج از نیاز سازمان است غیرفعال کند.

۵-۸ پس از نصب و راه‌اندازی محصول باید آموزش‌های لازم برای بهره‌برداری از تمام قابلیت‌های محصول به سازمان ارائه شود.

۵-۹ پس از نصب و راه‌اندازی محصول باید صورتجلسه تحویل محصول با ذکر تمامی قابلیت‌های ارائه شده و مسئولیت‌های طرفین در قبال آن‌ها تنظیم شده و به تایید طرفین برسد.

## ۶- الزامات پشتیبانی

۶-۱ ارائه‌کننده باید آسیب‌پذیری محصول و اجزای مستقل بکار رفته در محصول خود را به طور مستمر رصد نماید و در صورت وجود آسیب‌پذیری بدون قید و شرط داشتن قرارداد پشتیبانی، به محض کشف آن از طریق کانال ارتباطی امن به سازمان‌های سازمان اطلاع‌رسانی شود و سپس ظرف ۷۲ ساعت یک راهکار کوتاه‌مدت برای پیشگیری از بروز خرابی یا حملات احتمالی ناشی از آسیب‌پذیری در اختیار آن‌ها قرار گیرد. ارائه‌کننده باید به سازمان‌های دارای قرارداد پشتیبانی، وصله امنیتی و راهنمای کامل استفاده از آن را طبق زمان مورد توافق در تفاهم‌نامه سطح خدمات، ارائه و از نصب آن اطمینان حاصل کند و به مابقی سازمان‌ها نیز اطلاع‌رسانی از انتشار وصله امنیتی انجام شود.

۶-۲ ارائه کننده باید در زمان ارائه بروزرسانی‌ها، وصله‌های امنیتی و تغییرات پیکربندی، ابتدا تغییرات را در محیط تست سازمان پیاده سازی نموده و پس از اطمینان از صحت عملکرد آن، در محیط عملیاتی سازمان اعمال نماید.

۶-۳ ارائه‌کننده در محصولات پورتال‌های سازمانی و سیستم مدیریت محتوی، مکانیزم تشخیص حملات Deface را تا حد امکان و مکانیزم جلوگیری از تغییر در فایلها و پایگاه داده را فراهم نماید و در اختیار سازمان قرار دهد.

۶-۴ در صورتی‌که ارائه‌کننده به هر دلیلی، قصد پشتیبانی محصول را نداشته باشد باید حداقل یک سال قبل از اتمام زمان خدمات پشتیبانی به کلیه سازمان‌ها اعلام نماید. این بند ناقض ماده شماره ۴-۲ نمی باشد.

## ۷- الزامات پایان قرارداد

۷-۱ ارائه کننده باید حداقل یک ماه قبل از پایان قرارداد رسما خاتمه قرارداد را به سازمان اطلاع دهد.

## ۸- ارتباطات با مرکز افتا

۸-۱ ارائه‌کننده، فهرست سازمان‌های استفاده کننده از محصول خود به همراه مشخصات نماینده فنی سازمان و نسخه و شناسه محصول تحویل داده شده به سازمان، به همراه گزارش آسیب‌پذیری‌های کشف شده در محصول و اقدامات انجام شده برای رفع آنها را به صورت گزارش‌های فصلی برای مرکز افتا ارسال نماید.

۸-۲ ارائه‌کننده اطلاعات ارتباطی با مرکز افتا شامل مشخصات و نحوه برقراری ارتباط با مدیرعامل، مدیر محصول و مسئول امنیتی محصول را جهت مدیریت رسیدگی به رخدادها به مرکز افتا اعلام نماید و در صورت تغییر در این اطلاعات، مشخصات بروز شده را به این مرکز ارسال نماید.

۸-۳ در صورت اطلاع از آسیب‌پذیری بحرانی در محصول و برای مدیریت رخدادها، لازم است تا شرکت در سریع ترین زمان ممکن، ارائه کننده محصول وجود آسیب‌پذیری را به این مرکز اعلام نماید.