شماره : ۸۰۸۸۶۱۶
تاریخ : ۱۴۰۵/۴/۲۰
پیوست :

جمهوری اسلامی ایران
وزارت صنعت، معدن و تجارت
سازمان حمایت مصرف‌کنندگان و تولیدکنندگان

بسمه تعالی

قرارداد خرید مجوز بهره‌برداری سامانه نرم‌افزاری SSO پلاس

مقدمه:

این قرارداد با توجه به اعلام عمومی این سازمان در تاریخ ۱۴۰۵/۰۱/۲۲ جهت خریداری و پیاده‌سازی سامانه نرم‌افزاری احراز هویت یکپارچه (Single Sign On (SSO از طریق پنجره واحد خدمات دولت هوشمند و پنجره واحد دستگاه هوشمند در سامانه تدارکات الکترونیک (ستاد ایران) براساس قسمت (ب) بند۱ مصوبه وزیران به شماره ۳۶۸۵۱/ت۶۲۵۲۱/ه مورخ ۱۴۰۳/۰۳/۰۱ فی مابین اشخاص ذیل منعقد گردید.

قرارداد حاضر فی‌مابین:

سازمان حمایت مصرف‌کنندگان و تولیدکنندگان به کد اقتصادی ۴۱۱۱۱۱۴۸۴۴۴۳ و به شماره ثبت ۳۳۰۳۶ و شناسه ملی ۱۰۱۰۰۷۸۴۷۰۱ به نشانی: تهران، خیابان ولیعصر، روبروی پارک ملت، خیابان صداقت (انصاری)، نبش مهرشاد، پلاک۶۶ - کد پستی: ۱۹۶۷۸۳۴۷۱۳ تلفن: ۲۲۰۵۸۳۵۶ به نمایندگی آقای حسین فرهیدزاده با سمت معاون وزیر و رئیس سازمان از طرف دیگر به‌عنوان **خریدار** و **شرکت دانش بنیان راهبرد امن ماهان** به کد اقتصادی ۱۴۰۱۳۳۵۸۶۵۲ و شماره ثبت ۶۳۱۵۱۴ به شناسه ملی ۱۴۰۱۳۳۵۸۶۵۲ به نمایندگی آقای سعید راحمی به عنوان مدیرعامل و آقای مهدی طهماسبی به عنوان رییس هیئت مدیره به نشانی تهران، خیابان کارگر شمالی، خیابان فرشی مقدم، پارک علم و فناوری دانشگاه تهران، ساختمان شماره ۲، طبقه ۱، واحد ۲۱۶ ،کد پستی ۱۴۳۹۸۱۳۲۰۶، تلفن ۸۶۰۹۵۸۷۰ از یک‌طرف به‌عنوان **فروشنده** منعقد می گردد. طرفین ملزم و متعهد به اجرای مفاد قرارداد و پیوست‌های آن که جزء لاینفک قرارداد می‌باشند، گردیدند:

ماده ۱ – موضوع قرارداد

موضوع قرارداد، عبارت است از خرید مجوز بهره برداری یک نسخه از سامانه SSO پلاس (که از این پس سامانه نامیده می شود) دارای گواهی ثبت نرم‌افزار نزد مرکز فناوری اطلاعات و رسانه های دیجیتال وزارت فرهنگ و ارشاد اسلامی به شماره ۱۰/۲۷۸۵ و گواهی تایید فنی نزد سازمان فناوری اطلاعات و ارتباطات به شماره ۲۰۶۹۱۱ و گواهی ثبت و احراز اصالت نرم‌افزار به شماره ش۲۰۷۵ صادره مورخ ۱۴۰۴/۰۸/۲۱ از سازمان فناوری اطلاعات و گواهی ارزیابی امنیتی

محصول به شماره AFTA-2014-PSA-0288 از مرکز مدیریت راهبردی افتا ریاست جمهوری و مطابق مشخصات فنی پیوست شماره ۱ و پیوست شماره ۲ که جزء لاینفک این قرارداد محسوب می شود، است.

ماده ۲ – مدت زمان قرارداد

۱-۲- مدت زمان نصب و پیکربندی موضوع قرارداد از تاریخ ۱۴۰۵/۰۴/۰۱ لغایت۱۴۰۵/۰۵/۰۱ به مدت ۱ ماه می باشد.

مدت زمان انجام فازهای مختلف پروژه به تفکیک زمان در جدول زمانی پیوست شماره۱ آمده است.

تبصره ۱) در شرایط خاص و در صورت تاییدخریدار مدت زمان اتمام قرارداد، می تواند به مدت یک ماه افزایش یابد.

تبصره ۲) پشتیبانی یکساله محصول.

ماده ۳ – درصدبندی پروژه

در رابطه با نحوه اجرای پروژه جدول درصدبندی پروژه به شرح ذیل می‌باشد:

جدول مبالغ قرارداد		
ردیف	عنوان	درصد از کل قرارداد
۱	نصب لایسنس (مجوز بهره برداری) یک نسخه از سامانه	٪۵۰
۲	پیکربندی سامانه	٪۳۰
۳	مشاوره و آموزش	٪۱۰
۴	گارانتی و پشتیبانی	٪۱۰
	جمع مبالغ	٪۱۰۰

ماده ۴ – مبلغ قرارداد و شرح نحوه پرداخت

هزینه خریداری کل موضوع قرارداد **۸,۳۰۰,۰۰۰,۰۰۰** ریال می باشد.

شرح نحوه پرداخت مطابق با جدول زیر می باشد:

ردیف	مرحله	توضیحات	تحویل دادنی‌های هر مرحله	زمان اجرا	درصد از کل قرارداد

۱	نصب سامانه	یک بار نصب لایسنس (مجوز بهره برداری) یک نسخه از سامانه SSO پلاس بر روی سرور کارفرما (لایسنس شبکه بیرونی)	نمایش منوهای سامانه	پس از عقد قرارداد	٪۵۰
۲	پیکربندی سامانه	• پیکربندی نسخه نصب شده : ○ اتصال به SSO دولت ○ اتصال به سرویس پیامک ○ تنظیم فرایند ورود به سامانه بر اساس U+O	ورود موفق به پنل کاربری و راهبری سامانه SSO پلاس بر اساس فرایند احراز هویت مستند در پیوست مشخصات فنی شماره ۱	پس از صورتجلسه تایید اتمام مرحله اول توسط کارفرما	٪۳۰
۳	مشاوره و آموزش	• ارسال مستندات راهنمای کاربری • ارسال مستندات راهنمای توسعه دهندگان • آموزش کاربری سامانه به مدت ۴ ساعت	• راهنمای کاربری • راهنمای توسعه دهندگان • دو جلسه آموزشی ۲ ساعته	پس از صورتجلسه تایید اتمام مرحله دوم توسط کارفرما	٪۱۰
۴	گارانتی و پشتیبانی رایگان	• رفع خطاهای احتمالی سامانه	• کارکرد صحیح سامانه	پس از صورتجلسه تایید اتمام مرحله سوم توسط کارفرما	٪۱۰

تبصره ۳) قرارداد مذکور مشمول قانون کار و سایر قوانین استخدامی نمی باشد.

تبصره ۴) ۵٪ به عنوان بیمه قرارداد کسر و پس از ارائه مفاصاحساب به شرکت پرداخت می‌گردد. همچنین ۱۰٪ به عنوان حسن انجام از هر صورتحساب کسر می‌گردد که پس از پایان قرارداد و تایید خریدار به فروشنده عودت داده می‌گردد.

تبصره ۵) ماموریت، اضافه کار ساعتی، پاداش پایان کار، عیدی و مرخصی به این قرارداد تعلق نمی‌گیرد.

تبصره ۶) خریدار می تواند در طول مدت قرارداد، به میزان افزایش یا کاهش حجم کار و متناسب با آن مبلغ قرارداد را تا سقف ۲۵٪ (بیست و پنج درصد) افزایش یا کاهش دهد.

تبصره ۷) به موجب قانون مالیات بر ارزش افزوده، در تمامی صورتحساب‌های صادره توسط فروشنده، درصد تعیین شده توسط سازمان امورمالیاتی (۱۰٪)، به عنوان مالیات بر ارزش افزوده(با ارائه گواهی مربوطه) محاسبه و به حساب فروشنده واریز می گردد.

ماده ۵ – تضمین ها

۵-۱- ۱۰٪ مبلغ کل قرارداد به عنوان ضمانتنامه بانکی به عنوان حسن انجام تعهد می‌بایست تحویل خریدار گردد.

۵-۲- در صورتیکه فروشنده به تشخیص خریدار از ایفای به موقع تمام یا قسمتی از تعهدات قراردادی، ظرف مواعد مقرر فازهای ماده ۳ قرارداد، خودداری و یا به تشخیص خریدار مرتکب تأخیر، تسامح، تساهل و قصور گردد، خریدار بدون نیاز به مراجعه به هر مرجع و انجام هرگونه مکاتبه، محق به ضبط ضمانت نامه مذکور و وصول مبالغ آن است.

۵-۳- چنانکه فروشنده تعهدات خود را به اتمام نرساند خریدار می‌تواند تضمین‌های مالی را به نفع دولت برداشت کند.

ماده ۶ –خدمات مازاد

در صورتی که خریدار نیازی به ارائه خدمات مازاد بر مراحل ماده ۴ قرارداد توسط فروشنده داشته باشد، فروشنده متعهد است صرفا در محدوده مشخص شده در پیوست خدمات فنی شماره ۱ نسبت به ارائه خدمت در قالب درخواست تغییرات و به ترتیب ذیل اقدام نماید:

۱. بررسی امکان پذیری درخواست
۲. برآورد هزینه انجام کار در صورت امکان‌پذیری
۳. تایید هزینه توسط خریدار
۴. برآورد زمان انجام کار
۵. تایید زمان انجام کار توسط خریدار
۶. انجام تغییرات مطابق با زمانبندی اعلام شده توسط فروشنده
۷. تحویل تغییرات در محیط آزمایشگاهی و امضاء صورتجلسه تحویل توسط خریدار
۸. تایید صورتحساب انجام تغییرات توسط خریدار
۹. نسخه گذاری در محیط عملیاتی توسط فروشنده

هزینه نفر/ساعت خدمات مازاد مطابق با تعرفه نظام صنفی رایانه‌ای سال قرارداد محاسبه می گردد.

ماده ۷ -تعهدات فروشنده

۱-۷- فروشنده متعهد گردید، حداکثر ۷ روز کاری پس از ابلاغ رسمی قرارداد، یک نفر را به عنوان نماینده تام الاختیار خود معرفی کند.

۲-۷- فروشنده متعهد گردید، طبق مرحله ۱ از ماده۴، پس از ابلاغ قرارداد، یک نسخه از سامانه را مطابق با مشخصات فنی پیوست قرارداد، روی یک سرور در محیطی که توسط خریدار تامین شده است، نصب کند.

۳-۷- فروشنده متعهد گردید، طبق مرحله ۲ از ماده ۴، پس از صورتجلسه تایید اتمام مرحله اول توسط کارفرما ، نسبت به پیکربندی سامانه مطابق با مرحله ۲ اقدام نماید.

تبصره ۸) در صورت گذشت ۱ ماه از مرحله اول و عدم ارائه سرویس‌های لازم جهت پیکربندی توسط خریدار ، سامانه با تنظیمات اولیه پیکربندی خواهد شد، سپس فاکتور مربوطه (مرحله ۲ از ماده ۴) صادر خواهد شد و عدم ارائه سرویس‌ها از سوی خریدار مانعی برای صدور و پرداخت صورتحساب مرحله دوم از ماده ۴ به فروشنده نیست.

۴-۷- فروشنده متعهد گردید، پس از صورتجلسه تایید اتمام مرحله دوم توسط کارفرما ، مطابق با مرحله ۳ از ماده ۴، نسبت به ارائه مستندات و برگزاری ۲ دوره آموزشی به مدت ۲ ساعت به صورت آنلاین یا حضوری اقدام نماید.

۵-۷- با اتمام مرحله سوم از ماده ۵، دوره گارانتی (پشتیبانی رایگان) سامانه آغاز می‌شود، خدمات پشتیبانی در دوره گارانتی انجام می‌شود و فروشنده متعهد است پس از اخذ صورتجلسه تایید اتمام مرحله سوم از خریدار (آغاز دوره گارانتی) خطاهای احتمالی سامانه را بررسی و رفع نماید.

۶-۷- فروشنده متعهد گردید، از اطلاعات خریدار که در طول قرارداد به دست می‌آید، حفاظت کند و آن‌ها را بدون اجازه خریدار به هیچ شخص یا سازمان دیگری منتقل نکند. فروشنده باید از استانداردهای امنیتی مناسب برای نگهداری و انتقال اطلاعات استفاده کند و در صورت بروز هرگونه نقض، به خریدار اطلاع دهد.

۷-۷- فروشنده متعهد گردید، در طول دوره پشتیبانی هرگونه باگ (خطا) سامانه را پس از اعلام خریدار ، بررسی و در صورتی که ناشی از عملکرد سامانه باشد، مطابق با زمانبندی رفع نماید.

۸-۷- فروشنده متعهد گردید، بستر و طریق مناسبی را جهت گزارش خطا، ثبت درخواست‌های پشتیبانی، مکاتبات و پاسخ به آن‌ها را با خریدار فراهم کند و ارتباط از این طریق رسمی تلقی خواهد شد.

۹-۷- فروشنده اعلام می‌نماید بازسازی اطلاعات صدمه دیده که به دلیل اشکالات سخت افزاری و یا ویروس‌های کامپیوتری و یا عوامل فورس ماژور حادث شده باشد، شامل این قرارداد نمی‌باشد.

۱۰-۷- فروشنده متعهد به نصب، پیکربندی و آموزش موضوع قرارداد از طریق دسترسی‌های لازم از راه دور که توسط کافرما ارائه شده اقدام نماید.

۱۱-۷- چنانچه فروشنده به منظور ایجاد تغییرات و بهینه‌سازی‌ها نیازمند قطع و یا اختلال در سرویس بود، می‌بایست موضوع را به اطلاع خریدار رسانده و تائید انجام کار را اخذ نماید.

۱۲-۷- پیمانکار نسبت به شناسایی و رفع آسیب‌پذیری های مکشوفه و یا ابلاغی به سرعت رسیدگی و اقدام نماید. همچنین رعایت امنیت داده، امنیت سامانه و نگهداری ضروری است.

ماده ۸- تعهدات خریدار

۱-۸- خریدار متعهد گردید، حداکثر ۷ روز پس از شروع قرارداد، یک نفر را به عنوان نماینده تام الاختیار خود برای همکاری، پیشبرد پروژه، تحویل و تایید مراحل پروژه و صورتحساب‌های فروشنده معرفی کند.

۲-۸- خریدار متعهد گردید، زیرساخت‌های لازم و صحیح برای نصب و راه‌اندازی و نگهداری سامانه طبق مشخصات فنی پیوست قرارداد را فراهم کند.

۳-۸- خریدار متعهد گردید، مطابق با مراحل ماده ۴، صورتحساب‌هایی که توسط فروشنده برای هر مرحله از قرارداد ارسال می‌شوند را ظرف مدت ۲۰ روز کاری، پس از تایید خریدار به حساب فروشنده واریز کند.

تبصره ۹): در صورت عدم پایبندی خریدار به تعهدات مالی خود در زمان مقرر، فروشنده مسئولیتی در قبال پشتیبانی از سامانه و تعهدات مندرج در این قرارداد ندارد.

۴-۸- خریدار متعهد گردید، محل و دسترسی‌های لازم و از راه دور امن را برای راهبری سامانه طبق مشخصات فنی پیوست قرارداد در اختیار فروشنده قرار دهد.

۸-۵- خریدار متعهد گردید، حداکثر طی ۷ روز کاری به درخواست‌ها، مکاتبات، دمو یا تحویل هر مرحله از قرارداد، بازخورد یا پاسخ های خود را به فروشنده به صورت مکتوب یا کانال ارتباطی معرفی شده توسط فروشنده، اعلام کند، در صورت عدم بازخورد ظرف این مدت، درخواست‌های فروشنده تایید شده تلقی خواهد شد.

۸-۶- خریدار متعهد گردید، در صورت نیاز به تغییرات در سامانه یا هر نوع درخواست خدمات مازاد، آن را به صورت کتبی به فروشنده اعلام کند. فروشنده صرفا در محدوده مشخص شده در پیوست خدمات فنی شماره ۱ و در صورت امکانپذیری، هزینه و زمان لازم برای انجام درخواست را به خریدار اعلام نماید. خریدار باید در مدت ۵ روز کاری، تایید یا رد هزینه و زمان و روش پرداخت را به فروشنده اطلاع دهد. در صورت توافق، فروشنده باید تغییرات را انجام دهد و صورتحساب مربوطه را برای خریدار ارسال کند.

۸-۷- خریدار متعهد گردید، مسئولیت یکپارچه‌سازی سامانه با سایر سیستم‌های موجود در محل خود را بر عهده بگیرد و همچنین در صورت هرگونه تغییر در شرایط سامانه و زیرساخت، قبل از اقدام، هماهنگی لازم را با فروشنده انجام دهد، در صورتی که تغییر، معماری استقرار را تحت تاثیر قراردهد باید در قالب درخواست تغییرات با فروشنده توافق گردد.

۸-۸- در صورتی که وقوع رویدادی به عنوان بروز خطای نرم افزار به فروشنده ارجاع شود، اما در جریان رسیدگی مشخص شود دلیل وقوع رویداد، خطای نرم افزار نبوده و دلایل دیگری از قبیل مدیریت یا کاربری ناصحیح نرم افزار، اختلالات سخت افزار و شبکه و ... دلیل امر بوده است، تعهدات زمانی از فروشنده ساقط شده و زمان صرف شده جهت رسیدگی، به عنوان خدمات مازاد منظور خواهد شد.

۸-۹- خریدار متعهد می گردد در طول مدت قرارداد و پس از آن مطابق با ماده ۶۲ قانون تجارت الکترونیک و ماده یک قانون حمایت از حقوق پدید آورندگان نرم افزارهای رایانه ای مصوب ۱۳۷۹ و آیین‌نامه اجرایی مصوب ۱۳۸۳، تحت هیچ شرایطی به طور مستقیم یا غیرمستقیم با و یا بدون واسطه اشخاص ثالث به حقوق مادی و معنوی فروشنده از جمله حق تألیف خسارت وارد ننماید و تحت هیچ شرایطی امکان دسترسی افراد ثالث را به محیط اجرایی و ساختار پایگاه داده ها را فراهم نیاورد.

ماده ۹-مالکیت

۹-۱- حق امتیاز (کپی رایت) (حقوق مالکیت اثر) سامانه موضوع قرارداد متعلق به فروشنده است. در عین حال، به موجب این قرارداد، یک مجوز با محدوده استفاده از یک نسخه اجرایی از سامانه مطابق شرایط قرارداد و مشخصات

سامانه، پس از تسویه حساب قرارداد، به خریدار تعلق می گیرد. این مجوز (لایسنس) صرفاً برای بهره برداری از یک نسخه از سامانه و صرفاً به منظور استفاده در یک سازمان مورد نظر خریدار بوده و هیچ شخص حقیقی و حقوقی دیگری، اجازه نصب یا استفاده از این نسخه را ندارد.

۲-۹- تحویل کد منبع (Source) سامانه جزء تعهدات موضوع قرارداد نمی‌باشد.

۳-۹- خریدار و کارکنان وی حق تکثیر، توزیع، نشر، واگذاری یا تغییر، برگردان کد منبع (Source) سامانه یا ماشین سرور اجرایی سامانه یا هر اقدام دیگری که ناقض حقوق پدیدآورنده نرم افزار باشد را ندارند و در صورت نقض، خریدار ملزم به جبران خسارت می‌باشد.

۴-۹- نام و نشان تجاری سامانه جزیی از سامانه و تحت پوشش حقوق مالکیت اثر بوده و خریدار متعهد به حفظ کامل نام و نشان تجاری فروشنده بر روی نرم‌افزار، صفحات و ملحقات آن به همان صورت که از سوی فروشنده ارائه می‌شود، می باشد.

ماده ۱۰-پشتیبانی

۱-۱۰- تعاریف :

- پشتیبانی نرم‌افزار: مجموعه‌ای است از خدمات، فعالیتها و تعهدات مشخص با هدف حصول اطمینان از کارکرد صحیح نرم‌افزار در حال استفاده و بهره‌برداری، بر اساس کارکردهای تعهد و توافق شده در زمان خرید نرم افزار.
- خطا (BUG): به معنی خطای برنامه‌نویسی است که در محیط سالم عاری از هرگونه ویروس و تداخل با سایر زیرساخت‌های اجرایی (مانند نرم‌افزار و سخت‌افزار) بروز می کند. خطا، ناشی از کدهای برنامه‌نویسی شده و مولفه‌های استفاده شده یا توسعه داده شده توسط پیمانکار است.

۲-۱۰- خطاهایی که ناشی از عملکرد ناصحیح دیگر سامانه‌ها باشد مشمول این قرارداد نمی گردد.

۳-۱۰- خدمات توسعه و شخصی سازی سامانه و خدماتی که به منظور دریافت مجوزهایی که به درخواست خریدار انجام می گیرد شامل خدمات پشتیبانی نبوده و در صورت امکان‌پذیری در قالب خدمات مازاد به صورت نفر/ساعت محاسبه و انجام خواهد شد.

۴-۱۰-کلیه خدمات پشتیبانی در روزهای کاری و ساعات اداری قابل بررسی است و درخواستهایی که در روزها و ساعات غیر اداری توسط خریدار داده شود، در صورت امکان‌پذیری به عنوان خدمات مازاد در نظر گرفته می‌شود.

۱۰-۵- پس از اتمام قرارداد، فروشنده در قالب قرارداد مستقل برای هر سال و با قیمت توافقی، خدمات پشتیبانی نرم‌افزار را ارائه می‌نماید.

۱۰-۶- اعلام خطا بر عهده خریدار می‌باشد و طی گزارشی از طریق کانال ارتباطی که با توافق طرفین ایجاد می‌گردد به فروشنده اطلاع داده می‌شود. همچنین فروشنده متعهد است پس از اعلام خطا توسط خریدار، ابتدا منشاء خطا را بررسی و مشخص نماید و در صورتی که منشاء خطا سیستم نرم‌افزاری باشد، نسبت به رفع خطا اقدام نموده و وضعیت را از طریق کانال ارتباطی به اطلاع خریدار برساند.

۱۰-۷- در صورتی که خریدار خطایی را اعلام کند و پس از بررسی فروشنده مشخص شود که منبع خطا مربوط به زیرساخت خریدار یا عواملی است که به نرم‌افزار یا خدمات فروشنده ارتباطی ندارد، هزینه بررسی و تشخیص خطا توسط فروشنده در قالب یک صورتحساب به خریدار اعلام می‌شود. خریدار موظف است این صورتحساب را بدون هیچ قید و شرطی در وجه فروشنده پرداخت نماید.

۱۰-۸- تمامی درخواست‌ها یا اعلام خطاها از سوی خریدار باید از طریق یک کانال ارتباطی مشخص صورت گیرد. فرآیند رسیدگی به درخواست‌ها یا خطاها شامل مراحل زیر است:

- اعلام درخواست یا خطا توسط خریدار
- بررسی اولیه توسط فروشنده
- اعلام هزینه انجام کار (در صورت وجود هزینه)
- تایید خریدار بر انجام کار
- انجام کار یا رفع خطا توسط فروشنده

۱۰-۹- در صورتی که خریدار به هر دلیل نیاز به انجام یک کار فوری داشته باشد (منظور از کار فوری، کارهایی است که نیاز به انجام در یک روز یا کمتر از یک روز دارند)، خریدار موظف است دسترسی لازم برای انجام کار از راه دور را در اختیار فروشنده قرار دهد. در غیر این صورت، فروشنده هیچگونه الزامی برای انجام درخواست فوری نخواهد داشت.

ماده ۱۱- ارزیابی آسیب‌پذیری و آزمون نفوذ

۱۱-۱- تعاریف:

آزمون نفوذ: آزمون نفوذ امنیتی به فرآیند شناسایی آسیب‌پذیری‌های موجود در سامانه اطلاق می‌شود که توسط تیم‌های تخصصی امنیتی و با استفاده از تکنیک‌ها و ابزارهای مختلف انجام می‌شود. این آزمون به‌منظور ارزیابی مقاومت سیستم در برابر تهدیدات امنیتی انجام شده و شناسایی آسیب‌پذیری‌ها به معنای وجود خطا یا نقص در عملکرد نرم‌افزار نیست.

۲-۱۱- شرایط آزمون امنیت:

- موارد با اهمیت کریتیکال و بالا: در صورت شناسایی آسیب‌پذیری‌هایی با درجه اهمیت بحرانی (Critical) و بالا (High) ، این موارد در طول مدت قرارداد تنها یکبار توسط فروشنده بررسی و قابل انجام خواهد بود.
- هزینه آزمون امنیت: تمامی هزینه‌های مرتبط با اجرای آزمون امنیت به عهده خریدار بوده و فروشنده هیچ‌گونه تعهدی برای پوشش این هزینه‌ها ندارد.
- آسیب‌پذیری‌ها به عنوان یافته‌های امنیتی: آسیب‌پذیری‌های شناسایی‌شده در آزمون نفوذ امنیتی به عنوان یافته‌های امنیتی در نظر گرفته می‌شوند و به عنوان خطا، نقص یا کاستی در عملکرد نرم‌افزار محسوب نمی‌شوند. فروشنده تنها متعهد به بررسی و رفع آسیب‌پذیری‌های با اولویت بحرانی و بالا خواهد بود.

ماده ۱۲-تعذر (فورس ماژور):

۱-۱۲- هر گاه بعلت حوادث قهری و غیر مترقبه هر یک از طرفین قرارداد نتوانند تعهدات خود را انجام دهد، عدم انجام تعهدات، نقض قرارداد تلقی نخواهد شد و پس از رفع آنها قرارداد به قوت خود باقی خواهد بود. جنگ، زلزله، سیل و طغیان‌های غیر عادی، که ناشی از کار فروشنده نباشد، جزو حوادث قهری محسوب شده و در مورد خسارات ناشی از آن‌ها به ترتیب زیر عمل خواهد شد:

۱-۱-۱۲- هر یک از طرفین در صورت بروز شرایط فورس ماژور باید موضوع را به اطلاع طرف دیگر برساند. خریدار با همفکری فروشنده تدابیر لازم را اتخاذ خواهد نمود. در طول مدت تعذر فروشنده موظف است حداکثر تلاش خود را در جهت حفظ اقدامات انجام شده و مدارک تهیه شده به بهترین نحو مطلوب و با کمترین تاخیر بعمل آورد.

۲-۱-۱۲- چنانچه مدت فورس ماژور بیش از سه ماه طول بکشد، در آن صورت هر یک از طرفین چنانچه تمایل داشته باشند، اختیار فسخ قرارداد با ارائه یادداشت کتبی را دارد. در این شرایط فروشنده محق به دریافت هزینه‌ها و

مخارجی است که تا آن زمان در ارتباط با عملیات موضوع قرارداد انجام داده است، بصورت توافقی تصمیم گیری خواهند کرد.

تبصره ۱۰): افزایش قیمت سیستم، قطعات یا سطح دستمزدها ، تورم، تغییر برابری نرخ ارزها وموارد دیگر از این قبیل تحت هیچ عنوان جزو موارد حوادث قهریه محسوب نخواهد شد.

ماده ۱۳-فسخ قرارداد

قرارداد در شرایط ذیل قابل فسخ می‌باشد:

۱-۱۳- خریدار در موارد زیر بدون نیاز به هر مرجعی می تواند قرارداد را فسخ و به فروشنده ابلاغ نماید و فروشنده حق هر گونه اعتراضی را از خود سلب و ساقط می‌نماید.

۱-۱-۱۳- در شرایطی که فروشنده به تشخیص خریدار نتواند نسبت به تکمیل و انجام کل یا بخشی از تعهدات خود مطابق مفاد قرارداد و بر طبق برنامه زمانی عمل نموده و نسبت به رفع نقایص اعلامی ظرف مدت دو هفته از دریافت اعلام خریدار اقدام نکرده باشد.

۲-۱-۱۳- چنانچه به تشخیص خریدار، فروشنده از انجام تمام یا قسمتی از تعهدات قراردادی، امتناع و خودداری نموده و یا در انجام آن مرتکب تساهل، تسامح و تأخیر (بیش از هفت روز) گردیده یا نسبت به رفع نقص یا نقایص حداکثر ظرف ۱۵ روز از تاریخ اعلام خریدار (از طریق فاکس ،ایمیل ،تلفن و غیره) اقدام ننماید.

۳-۱-۱۳- در صورتی که فروشنده اعلام ورشکستگی نموده و یا اینکه به تشخیص خریدار قادر به انجام تعهدات خود نباشد.

۴-۱-۱۳- چنانچه شرکت فروشنده منحل گردیده و یا درخواست انحلال نماید.

۲-۱۳- طرفین در موارد ذیل حق فسخ قرارداد و ابلاغ آن به طرف دیگر را دارند :

الف) بر اساس توافق کتبی طرفین

ب) بر اساس اختیار هر یک از طرفین در صورتی که مدت فورس ماژور ایجاد شده از سه ماه طولانی‌تر گردیده باشد.

۳-۱۳- در صورت استفاده از اختیارات مقرر ذکر گردیده در فسخ قرارداد ، خریدار این اجازه را خواهد داشت که وجه حسن انجام کار و همچنین مبالغی را که از صورتحساب‌های فروشنده، به هر دلیلی تا زمان فسخ قرارداد کسر کرده است

(در صورت وجود)، بدون خدشه وارد آوردن به حقوق خود برای مطالبه خسارات، غرامت و دریافت هر هزینه و یا مخارجی که برای جبران زیان‌های وارده، لازم است، به نفع خود ضبط و برداشت نماید.

۴-۱۳- چنانچه فسخ بر مبنای توافق کتبی صورت گیرد طرفین در مورد چگونگی نحوه تسویه حساب توافق خواهند نمود.

۵-۱۳- با دریافت اعلام فسخ قرارداد، با هر یک از روش‌های فوق فروشنده ارائه خدمات را متوقف کرده و از پذیرش تعهد برای شروع هر کار جدید در ارتباط با خدمات یاد شده خودداری کرده و چنانچه درخواست شود هر تلاش معقولی را برای فسخ کلیه تعهدات جاری بر اساس شرایط مورد رضایت خریدار، فراهم می‌نماید و بعد از آن فقط اقداماتی را انجام خواهد داد که ممکن است برای حفظ و نگهداری اقداماتی که قبلاً انجام داده، ضروری باشد، و در طی یک مدت معقول بعد از تاریخ اعلام فسخ، فروشنده گزارش نهایی اقدامات انجام شده خود را مستنداً به خریدار ارائه خواهد کرد.

تبصره ۱۱): اعلام کتبی از سوی هر یک از طرفین به نشانی اعلامی طرف مقابل از طریق پست پیشتاز به منزله ابلاغ قانونی بوده و دیگر نیازی به اعلام مراتب از طریق اظهارنامه رسمی نیست.

ماده ۱۴- حل‌وفصل اختلافات

۱-۱۴- طرفین قرارداد باید نهایت کوشش خود را برای حل اختلاف احتمالی فیمابین در رابطه با موضوع این قرارداد از طریق مذاکره و حل مسالمت آمیز به کار گیرند.

۲-۱۴- هرگاه اختلاف ناشی از این قرارداد را که نتوان ظرف مدت یک ماه از طریق مذاکره حل نمود ذینفع می تواند مراتب را از طریق مراجع ذیصلاح قضایی پیگیری نماید.

۳-۱۴- مادامی که موضوع اختلاف در حال بررسی است و به تصمیم قطعی منتهی نگردیده، طرفین باید به تعهدات خود در این تعهد نامه ملتزم بوده و آن را اجرا نمایند.

ماده ۱۵- قوانین حاکم برقرارداد

قوانین و مقررات حاکم بر این قرارداد، قوانین و مقررات جاری کشور می‌باشد.

ماده۱۶- اخطار و نشانی

نشانی طرفین که در صدر قرارداد درج گردیده به منزله اقامتگاه قانونی طرفین می باشد، لذا مکاتبات رسمی و ارسال مراسلات از طریق نشانی‌های فوق قانونی تلقی می‌شود. درصورت تغییر نشانی طرفین موظف هستند ظرف مدت ۱۵ روز

کاری مراتب را به طرف مقابل اطلاع دهند، در غیر اینصورت کلیه مکاتبات صورت گرفته با نشانی های فوق قانونی تلقی شده و عذر عدم اطلاع پذیرفته نخواهد شد.

ماده۱۷- مواد و نسخ

این قرارداد در ۱۷ ماده، ۱۱ تبصره و پیوست ۲۳ صفحه‌ای، در دو نسخه با اعتبار یکسان تهیه و کلیه شرایط مندرج در آن توسط امضاکنندگان زیر به دقت مطالعه گردیده و مورد توافق طرفین قرار گرفته و هرگونه تغییر در مفاد آن منوط به موافقت کتبی طرفین قرارداد می باشد.

"خریدار"	"فروشنده"
نام و نام خانوادگی: حسین فرهیدزاده سمت: معاون وزیر، رییس هیات مدیره ومدیرعامل سازمان	نام و نام خانوادگی: آقای سعید راحمی سمت: مدیرعامل شرکت دانش بنیان راهبرد امن ماهان
نام و نام خانوادگی: اسماعیل صیامی سمت: معاون توسعه مدیریت و منابع	
نام و نام خانوادگی: طالب زمزمی سمت: ذیحساب و مدیرکل امور [illegible]	نام و نام خانوادگی: آقای مهدی طهماسبی سمت: رییس هیئت مدیره شرکت دانش بنیان راهبرد امن ماهان

شرکت دانش بنیان
راهبرد امن ماهان
RAMCO
شماره ثبت ۶۳۱۵۱۴

سازمان حمایت مصرف کنندگان و تولید کنندگان
جمهوری اسلامی ایران
وزارت صنعت، معدن و تجارت

نام و نام خانوادگی: مهرداد ایزدی سمت: مدیر کل دفتر بررسی های اقتصادی ،فناوری اطلاعات و امنیت فضای مجازی(ناظر قرارداد)	

پیوست شماره(۱) قرارداد
(جدول زمانبندی اجرا)

ردیف	شرح مختصر از مراحل اجرایی	جدول زمانی انجام مراحل به هفته
۱	نصب و راه‌اندازی	
۲	آموزش	
۳	آغاز یکپارچه‌سازی سامانه‌ها با SSO	

پیوست شماره(۲) قرارداد
(مشخصات فنی)

پیوست فنی قرارداد برای مشخصات فنی و جزو لاینفک قرارداد است: محصول نرم افزار آماده اس اس او پلاس (SSO Plus)

است که از این پس سامانه نامیده می شود. موضوع قرارداد، واگذاری حق بهره‌برداری غیرانحصاری از یک نرم‌افزار آماده با نام SSOپلاس می‌باشد و این قرارداد ناظر بر تولید نرم‌افزار سفارشی نمی‌باشد و کلیه قابلیت‌ها، محدودیت‌ها و تعهدات فنی صرفاً در چارچوب مفاد این پیوست معتبر خواهد بود. SSO پلاس دارای گواهی ثبت نرم‌افزار نزد مرکز فناوری اطلاعات و رسانه های دیجیتال وزارت فرهنگ و ارشاد اسلامی به شماره ۱۰/۲۷۸۵ و گواهی تایید فنی نزد سازمان فناوری اطلاعات و ارتباطات به شماره ۲۰۶۹۱۱ و گواهی ثبت و احراز اصالت نرم‌افزار به شماره ش۲۰۷۵ صادره مورخ ۱۴۰۴/۰۸/۲۱ از سازمان فناوری اطلاعات و گواهی ارزیابی امنیتی محصول به شماره AFTA-2014-PSA-0288 از مرکز مدیریت راهبردی افتا ریاست جمهوری می‌باشد.

۱. تعاریف کلی:

۱،۱. سامانه = منظور، سامانه SSO پلاس است و گاها با اسامی زیر نیز شناخته می شود:

- Single Sign-On
- Identity Provider
- Authorization Server
- Identity Management

۱،۲. کلاینت یا سامانه تخصصی سازمان (طبق استاندارد OAuth) منظور سامانه/اپلیکیشن/نرم‌افزار تخصصی سازمان است که به سامانه SSO پلاس متصل می‌شود. طبق استانداردهای مذکور به کلاینت، Resource Server یا Relying Party هم گفته می‌شود.

۱،۳. کاربر منظور کاربر نهایی بهره بردار از سامانه است.

۱،٤. احراز هویت (Authentication): فرآیند ورود (Login) کاربر به سامانه SSO پلاس است.

۱،٥. مجوز ورود (Access) به کلاینت ها (سامانه تخصصی): منظور اجازه ورود به کاربران، نقش‌ها و گروه‌ها به کلاینت (سامانه تخصصی) توسط راهبر SSO است = چه کسی به کدام سامانه وارد شود.

۱،٦. مجاز شماری (Authorization): سامانه بر پایه نقش، گروه یا خصیصه کاربر توکن‌های Access Token، ID

Token، UserInfo را می‌سازد و طی JWT در claim ها در اختیار کلاینت‌ها می‌گذارد. کلاینت (همان سامانه تخصصی) با داشتن این اطلاعات می تواند از پروتکل های RBAC (Role-Based Access Control) و GBAC (Group-Based Access Control) و ABAC (Attribute-Based Access Control) در سامانه خودش استفاده نماید.

۲. استانداردهای سامانه مطابق استانداردهای OAuth2.0 و OIDC1.0 است.

۲،۱. استاندارد OAuth 2.0 Framework (RFC 6749):

- سامانه SSOپلاس با استفاده از پروتکل OAuth و OpenID Connect مکانیزم احراز هویت و دسترسی به سامانه های کاربردی و برنامه‌های مختلف را فراهم می کند.
- OAuth 2.0 یک استاندارد صنعت برای تفویض دسترسی یا Authorization است که به سامانه‌های تخصصی (کلاینت‌ها) امکان می‌دهد با کسب توکن‌های موقت به منابع کاربر در یک سرویس وب دسترسی محدوده‌دار پیدا کنند، بدون اینکه نیاز باشد نام‌کاربری و گذرواژه کاربر را مستقیماً در اختیار داشته باشند.
- این RFC شرح جامعی از پروتکل OAuth را ارائه می‌دهد. این استاندارد توضیح دقیقی از مراحل احراز هویت، صدور توکن‌های دسترسی، انواع مجوزها و تعاملات بین موجودیت‌ها (کلاینت، سرویس‌دهنده احراز هویت و سرویس‌دهنده منابع) را ارائه می‌دهد.

۲،۲. OpenID Connect 1.0

- یک لایهٔ احراز هویت Authentication مبتنی بر OAuth 2.0 است. OIDC با استفاده از جریان‌های OAuth (به‌ویژه Authorization Code Flow) امکان تأیید هویت کاربران را به صورت یکپارچه فراهم می‌کند. این پروتکل مفهومی به‌نام ID Token (توکن هویتی) را معرفی می‌کند که یک JWT JSON Web Token حاوی ادعاهای هویتی (claims) درباره کاربر است. به کمک ID Token و همچنین یک Endpoint اطلاعات کاربر (UserInfo)، کلاینت می‌تواند مشخصات پایه کاربر (مانند نام، ایمیل و ...) را به شکل استاندارد دریافت کرده و هویت کاربر را احراز کند. به بیان دیگر، OAuth 2.0 مجوز دسترسی صادر می‌کند و OpenID Connect روی همان بستر، تأیید هویت

کاربر را اضافه می‌کند.

۲,۳. OAuth 2.0 Bearer Token Usage (RFC 6750)

۲,٤. این RFC به جزئیات استفاده از توکن‌های حامل Bearer Tokens در پروتکل OAuth پرداخته و نحوه ارتباط بین کلاینت و سرویس‌دهنده منابع با استفاده از این توکن‌ها را توضیح می‌دهد.

۲,٥. The OAuth 2.0 Authorization Framework: JWT Profile (RFC 7523)

۲,٦. این RFC بر روی استفاده از JWT (JSON Web Tokens) در پروتکل OAuth تمرکز دارد. JWTها به عنوان توکن‌های دسترسی مورد استفاده قرار می‌گیرند.

۲,۷. JSON Web Token (JWT) (RFC 7519)

- این RFC به جزئیات استفاده از JWT به عنوان یک فرمت استاندارد برای نشانه‌گذاری Claims و اشتراک اطلاعات پرداخته و مشخصات و نحوه ایجاد و تجزیه‌تحلیل JWT را توضیح می‌دهد.

۲,۸. OAuth 2.0 for Native App (RFC 8252)

۲,۹. OAuth 2.0 Token Introspection (RFC 7662)

۲,۱۰. Proof Key of Code Exchange (RFC 7636)

۳. تغییرات: با توجه به الزام به رعایت تطابق با استانداردها، تغییرات در سامانه نرم‌افزار آماده SSO پلاس بسیار محدود و با رعایت امکان سنجی و تایید توسط تیم فنی فروشنده خواهد بود.

۳,۱. هرگونه درخواست تغییر در نرم‌افزار آماده SSO پلاس می‌بایست ابتدا توسط تیم فنی فروشنده مورد بررسی و امکان‌سنجی قرار گیرد.

۳,۲. در صورتیکه امکان سنجی انجام تغییرات توسط تیم فنی فروشنده مورد تایید باشد، هزینه انجام تغییرات و زمان‌بندی آن به کارفرما اعلام می‌گردد.

۳,۳. در صورتیکه هزینه انجام تغییرات و زمان‌بندی آن مورد تایید کارفرما قرار گیرد، فروشنده مطابق با زمان اعلام شده اقدام به انجام تغییرات خواهد کرد.

٤. روش نصب و راه اندازی سامانه به صورت ماشین مجازی روی بستر ESXi خواهد بود که توسط کارفرما باید تامین شود. نصب به صورت اجرای یک فایل OVA از پیش ساخته توسط تیم فنی SSO پلاس، انجام خواهد شد.

٥. تمامی خدمات، شامل نصب ،آموزش، مشاوره و خدمات گارانتی (حفظ پایداری سامانه و بررسی و رفع خطاهای احتمالی) و همچنین کلیه خدمات مرتبط با سامانه SSO پلاس به صورت دسترسی از راه دور با ssh می‌باشد.

٦. پیش‌نیازهای فنی شامل تخصیص IP، تنظیم DNS، زمان‌بندی NTP، گواهی TLS معتبر، و دسترسی‌های لازم شبکه‌ای به سرویس‌های بیرونی (در صورت استفاده) است توسط کارفرما تامین خواهد شد.

۷. محدوده نصب سامانه یک بار روی یک سرور و در یک محیط عملیاتی خواهد بود.

۸. محدوده استفاده از سامانه برای کاربران بیرونی سازمان حمایت از مصرف کنندگان و تولید کنندگان می‌باشد.

۹. محدوده بهره برداری از سامانه برای استقرار در سازمان حمایت از مصرف کنندگان و تولید کنندگان خواهد بود و برای سازمان های بالاسری یا پایین دستی که شخصیت حقوقی دارند باید لایسنس جداگانه تهیه شود.

۱۰. اگر خریدار به هر علت از جمله تعدد نسخ سامانه برای گروه کاربری یا کلاینت های مختلف، یا شبکه های مختلف، درخواست نصب جداگانه‌ای داشته باشد، مستلزم تهیه لایسنس جداگانه و پرداخت هزینه آن خواهد بود. بدیهی است قیمت لایسنس جدیدبر مبنای استعلام قیمت جدید از SSOپلاس خواهد بود.

۱۱. یکپارچه سازی کلاینت‌ها یا همان سامانه‌های تخصصی سازمان با سامانه SSO در تعهدات تیم SSOپلاس نبوده و به عهده پیمانکاران سامانه‌های مقصد می‌باشد و فروشنده در این خصوص اسناد راهنما را در اختیار پیمانکاران مربوطه قرار خواهد داد.

۱۲. هر گونه خرابی سامانه که ناشی از دستکاری نادرست خریدار در محیط اجرا باشد، بایستی در یک توافق جداگانه مورد بررسی زمان و هزینه قرار گرفته و با توافق طرفین انجام شود.

۱۳. در صورت درخواست خریدار مبنی بر حضور فروشنده در محل خریدار ، هزینه ایاب و ذهاب و اقامت به عهده خریدار می‌باشد.

۱٤. تحویل دادنی های فروشنده به خریدار:

۱۴,۱. تحویل دسترسی راهبری اصلی سامانه: شناسه و رمز راهبری پنل سامانه اس اس او پلاس تحت وب (Administrator Account)

۱۴,۲. مستندات کاربری سامانه (User Guide)

۱۴,۳. مستند راهنمای توسعه‌دهندگان(Developer Guide)

۱۴,۴. مستندات خارج از موارد فوق مشمول هزینه جداگانه است.

۱۴,۵. تحویل دسترسی به سرور سامانه صرفا برای تنظیم آی پی و ریست کردن سرور سامانه است.

۱۵. نصب یا راه‌اندازی ایجنت روی سیستم عامل با تایید تیم فنی SSO پلاس انجام خواهد شد.

۱۶. پشتیبان گیری (Backup): پشتیبان گیری به عهده خریدارست و فروشنده در این زمینه همکاری خواهد نمود.

۱۷. حق امتیاز (کپی رایت) (حقوق مالکیت اثر) سامانه موضوع قرارداد متعلق به فروشنده است. در عین حال، به موجب این قرارداد، یک مجوز غیرانحصاری با محدوده استفاده مشروح از یک نسخه اجرایی از سامانه مطابق شرایط قرارداد و مشخصات سامانه، پس از تسویه حساب قرارداد، به خریدار تعلق می گیرد. این مجوز (لایسنس) صرفاً برای بهره برداری از یک نسخه از سامانه و صرفاً به منظور استفاده در یک سازمان مورد نظر خریدار بوده و هیچ شخص حقیقی و حقوقی دیگری، اجازه نصب یا استفاده از این نسخه را ندارد.

۱۸. تحویل کد منبع (Source) سامانه جزء تعهدات موضوع قرارداد نمی‌باشد وخریدار و کارکنان وی حق تکثیر، توزیع، نشر، واگذاری یا تغییر، برگردان کد منبع (Source) سامانه یا ماشین سرور اجرایی سامانه یا هر اقدام دیگری که ناقض حقوق پدیدآورنده نرم افزار باشد را ندارند و در صورت نقض، خریدار ملزم به جبران خسارت می‌باشد.نام و نشان تجاری سامانه جزیی از سامانه و تحت پوشش حقوق مالکیت اثر بوده و خریدار متعهد به حفظ کامل نام و نشان تجاری فروشنده بر روی نرم‌افزار، صفحات و ملحقات آن به همان صورت که از سوی فروشنده ارائه می‌شود، می‌باشد.

۱۹. فروشنده متعهد است در طول دوره پشتیبانی، به‌روزرسانی‌های جزئی سامانه را صرفاً در چارچوب قابلیت‌های نسخه خریداری‌شده و مطابق جدول مشخصات فنی این پیوست ارائه نماید. این به‌روزرسانی‌ها محدود به رفع خطاها، بهبودهای

امنیتی و اصلاحات فنی جزئی بوده و شامل توسعه‌های جدید، ماژول‌های اضافی یا هر گونه قابلیت خارج از فهرست مشخصات قراردادی نخواهد بود.

۲۰. لیست مشخصات، قابلیت‌ها و فرآیندهای نرم‌افزار خریداری شده به شرح ذیل است:

دسته بندی	تعریف	در محدوده قرارداد
پروتکل‌های اصلی	۱. OAuth2.0 شامل استانداردهای ۱،۱. RFC 6749 OAuth 2.0 Authorization Framework ۱،۲. RFC 6750 OAuth 2.0 Bearer Token Usage ۱،۳. RFC 6751 OAuth 2.0 Proof-Key for Code Exchange (PKCE) ۱،٤. RFC 7009 OAuth 2.0 Token Revocation ۱،٥. RFC 7662 OAuth 2.0 Token Introspection ۱،٦. RFC 8414 OAuth 2.0 Authorization Server Metadata ۲. OpenID Connect 1.0 ۳. JWT/JWS/JWK ۳،۱. RFC 7519 JSON Web Token (JWT) ۳،۲. RFC 7515 JSON Web Signature (JWS) ۳،۳. RFC 7517 JSON Web Key (JWK) ٤. استانداردهای عمومی مثل: https/TLS، CORS (با امکان تعریف Allowed-Origin برای هر کلاینت) و منطبق بر RFC 4648 URL encoding ٥. SAML2.0	در محدوده قرارداد است

انواع کاربر	۶. حقیقی و حقوقی	در محدوده قرارداد است
ایجاد کاربر	۷. اضافه، ویرایش و حذف کاربر توسط راهبر سامانه یا کاربری که نقش مدیریت کاربران را دارد خواهد بود، در این روش اقلام اطلاعاتی مستقیما توسط راهبر ثبت می‌شود و از ارتباطی با سرویس‌های استعلامی ندارد و مقادیر پروفایل کاربر با تنظیم راهبر خواهد بود. ۸. پروفایل کاربر شامل اقلام: نام کاربری، کد ملی، تاریخ تولد، شماره موبایل، شماره تلفن ثابت و ایمیل خواهد بود.	در محدوده قرارداد نیست
ایجاد کاربر	۹. تدارک کاربر (Just-in-Time Provisioning) از یک Active Directory (فقط-خواندنی) در این حالت، ایجاد، حذف و تغییر پروفایل و رمز کاربر بایستی در AD انجام شود و از طریق SSO پلاس نخواهد بود. تدارک کاربر در زمان لاگین کاربر خواهد بود، این الگو برای رعایت امنیت حداکثری در معماری استقرار سامانه است. SSO پلاس نباید به Power User از AD دسترسی داشته باشد، بنابراین رویکرد تدارک تدریجی کاربران خواهد بود نه همگام سازی. ۱۰. اقلام اطلاعاتی قابل استخراج از AD: شناسه کاربری، نام و نام خانوادگی، ایمیل و شماره موبایل است. در صورت وجود اقلام دیگر بایستی در قرارداد ذکر گردد.	در محدوده قرارداد نیست
ایجاد کاربر	۱۱. تدارک کاربر (Just-in-Time Provisioning) از یک منبع بیرونی (فقط-خواندنی) مانند بانک اطلاعاتی سازمانی (خارج از SSO ولی در محدوده سازمان)، در هربار لاگین کاربر پروفایل کاربر با بانک اطلاعاتی همگام سازی خواهد شد بنابراین منبع اصلی ایجاد کاربر و تغییر پروفایل کاربر بانک اطلاعاتی خارج از SSO پلاس خواهد بود.	در محدوده قرارداد نیست

	۱۲. اقلام اطلاعاتی قابل استخراج: شناسه کاربری، نام و نام خانوادگی، ایمیل و شماره موبایل است. در صورت وجود اقلام دیگر بایستی در قرارداد ذکر گردد.	
ایجاد کاربر	۱۳. امکان ثبت‌نام خودکار توسط کاربر (Self-Registration) از طریق سرویس‌های استعلام هویت ثبت احوال و شاهکار، اقلام اطلاعاتی ثبت نام کدملی، سپس شماره موبایل و تاریخ تولد خواهد بود. مراحل ثبت نام شامل: مرحله اول کدملی، مرحله دوم: تاریخ تولد، شماره موبایل، پس از استعلام موفق سرویس هویتی و شاهکار در مرحله سوم: وارد کردن کد OTP و مرحله چهارم: تنظیم رمز عبور خواهد بود. ۱٤. تامین سرویس های استعلامی با کارفرما خواهد بود.	در محدوده قرارداد نیست
ایجاد کاربر	۱۵. امکان ثبت‌نام خودکار توسط کاربر (Self-Registration) برای کاربران حقوقی از طریق سرویس استعلام ثبت احوال، شاهکار و اشخاص حقوقی، اقلام اطلاعاتی ثبت نام شناسه ملی شرکت، کد ملی مدیر عامل و تاریخ تولد و شماره موبایل مدیرعامل خواهد بود. ۱٦. تامین سرویس های استعلامی با کارفرما خواهد بود.	در محدوده قرارداد نیست
ایجاد کاربر	۱۷. ایجاد اولیه کاربران توسط تیم فنی SSO پلاس: پروفایل کاربر شامل اقلام: نام کاربری، کد ملی، تاریخ تولد، شماره موبایل، شماره تلفن ثابت خواهد بود. ۱۸. تیم فنی SSOپلاس می‌تواند بر اساس یک لیست اولیه بعد از مرحله پیکربندی سامانه نسبت به ایجاد کاربران یکبار اقدام نماید، اما استخراج، کانورت یا مهاجرت داده‌ها از سامانه‌های قدیمی به عهده کارفرما است.	در محدوده قرارداد نیست
ایجاد کاربر	۱۹. امکان ثبت‌نام کاربران از طریق Identity Provider دولت من خواهد بود	در محدوده قرارداد است

	که اقلام اطلاعاتی کاربران مطابق Token دولت من خواهد بود.	
ایجاد کاربر	۲۰. سرویس های استعلام هویت کاربر در زمان ثبت نام؟؟؟؟ شامل چه سرویس هایی؟؟ چه اقلام اطلاعاتی؟؟ و روش ارائه در Claims های JWT ۲۱. آیا باید در هر بار لاگین مجدد استعلام شود؟؟	در محدوده قرارداد نیست
روش احراز هویت (ورود)	۲۲. احراز هویت با شناسه کاربر و رمز عبور از SSO پلاس	در محدوده قرارداد نیست
روش احراز هویت (ورود)	۲۳. احراز هویت با شناسه کاربر و پیامک OTP. پیکربندی سرویس پیامک OTP یکبار در مرحله پیکربندی سامانه، بواسطه یک API ارسال پیامک که توسط کارفرما در اختیار تیم SSOپلاس قرار می گیرد، پیکربندی خواهد شد.	در محدوده قرارداد است
روش احراز هویت (ورود)	۲۴. احراز هویت ۲ عاملی: با شناسه کاربر و رمز عبور و پیامک OTP.	در محدوده قرارداد نیست
روش احراز هویت (ورود)	۲۵. تنوع فرآیند احراز هویت کاربران بین حالت های Username Password و Username OTP توسط راهبر قابل تنظیم خواهد بود.	در محدوده قرارداد نیست
روش احراز هویت (ورود)	۲۶. کاربر در قسمت OTP امکان وارد کردن کد Time-OTP خواهد داشت. ۲۷. TOTP توسط کاربر با اسکن QR-Code در پروفایل کاربری قابل تنظیم خواهد بود.	در محدوده قرارداد نیست

روش احراز هویت (ورود) قابلیت	۲۸. احراز هویت با شناسه و رمز کاربران وابسته به یک Active Directory	در محدوده قرارداد نیست
روش احراز هویت (ورود) قابلیت	۲۹. احراز هویت با شناسه و رمز کاربران وابسته به چند Active Directory مختلف (تعداد ؟؟)	در محدوده قرارداد نیست
روش احراز هویت (ورود) ملاحظات	۳۰. در احراز هویت ها با سرویس های بیرونی امکان ایجاد یا ویرایش اطلاعات کاربر باید در مخزن اصلی اطلاعات کاربران انجام شود. **در توضیحات باشد یا ملاحظات یا هر کدام از بخش ها** ۳۱. در حالتی که SSO پلاس کاربران را از طریق AD یا یک بانک داده بیرونی Provisiong کند، اضافه شدن (ثبت نام) کاربر در SSO پلاس به محض اولین اقدام موفق (Just In Time) کاربر برای لاگین خواهد بود. با رعایت این موضوع اگر مخزن بیرونی AD باشد، اولین تلاش کاربر برای احراز هویت باید با شناسه و رمز AD باشد تا امکان استعلام LDAP از AD امکان پذیر شود.	در محدوده قرارداد نیست
روش احراز هویت (ورود) ملاحظات	۳۲. آیا ورود کاربر وابسته به سرویس بیرونی است؟؟؟ چه سرویس هایی؟	ثبت نام کاربر وابسته به SSO دولت است و ورودهای بعدی کاربر وابسته به سرویس پیامکی است
پروفایل تکمیلی	۳۳. پروفایل تکمیلی برای مقادیر زیر در پروفایل فعال خواهد بود ۳۴. این مقادیر توسط کاربر نیز قابل ویرایش خواهد بود یا توسط راهبر سامانه	در محدوده قرارداد نیست

وریفای ایمیل در پروفایل	۳۵. سامانه قابلیت وریفای ایمیل با ارسال Email-OTP از SMTP را دارد. نتیجه وریفای بودن ایمیل در Access Token برای کلاینت ها قابل مشاهده خواهد بود.	در محدوده قرارداد نیست
مجوز ورود (Access)به کلاینت ها	۳۶. راهبر می‌تواند به ازای هر کلاینت، مجوز ورود را به کاربران، نقش‌ها و گروه‌های موجود در سامانه محدود نماید، این ساختار لیست سفید هم شناخته می‌شود (Whitelist). ۳۷. SSO پلاس بر اساس انتساب مستقیم کاربر یا نقش‌ها یا گروه‌ها مجوز دسترسی به سامانه را فراهم می‌نماید و نه ارث‌بری نقش ها و گروه‌ها.	در محدوده قرارداد است
گروه بندی خودکار	۳۸. قابلیت اضافه شدن خودکار کاربر به گروه در مدل‌های JIT Provisioning امکان پذیر است، به این صورت که شناسه کاربری احتمالی کاربر در گروهبندی خودکار تنظیم می‌شود و زمانی که اولین ورود کاربر انجام و حساب کاربری وی ساخته شود، در این گروه قرار خواهد گرفت (Auto-Grouping).	در محدوده قرارداد نیست
مجازشماری Authorization	۳۹. SSO پلاس، یک Identity Provider است که چارچوب RBAC و GBAC را برای کلاینت‌ها یا همان سامانه‌های تخصصی فراهم می‌کند. با قابلیت انتقال نقش‌ها و گروه‌ها به داخل توکن (Token Claims) جهت خوانش توسط کلاینت‌ها.	در محدوده قرارداد نیست
مجازشماری Authorization	۴۰. راهبر اصلی یا کاربری که نقش مدیریت نقش‌ها را داشته باشد می تواند نقش‌ها (Role) را تعریف، حذف و ویرایش کند. این نقش ها و گروه‌ها باید در SSO پلاس تعریف و مدیریت شوند و از منبع بیرونی Provisioning صورت نمی‌گیرد. ۴۱. راهبر یا کاربر دارای نقش مدیریت گروه، قابلیت تعریف گروه Group	در محدوده قرارداد نیست

	دارد. ۴۲. امکان انتساب نقش به گروه وجود دارد. ۴۳. امکان انتساب گروه به کاربر وجود دارد.	
مجازشماری Authorization	۴۴. تمام تصمیمات مجازشماری در سامانه‌های تخصصی در سطح توکن‌های JWT (Access Token، ID Token و UserInfo) انجام می‌شود؛ به‌طوری که ادعاهای (claims) مورد نیاز برای اعمال سیاست‌های دسترسی، به‌صورت استاندارد OIDC در توکن گنجانده می‌شوند.	در محدوده قرارداد نیست
مجازشماری Authorization	۴۵. راهبر قابلیت تعریف نقش‌های ترکیبی (Composite-Role) دارد. به عبارت دیگر، وقتی نقش A به‌عنوان نقش ترکیبی تعریف می‌شود و نقش A ترکیبی از نقش B، نقش C، ... می‌گردد؛ تمام ادعاهای (claims) نقش‌های B، C، ... به‌صورت خودکار در توکن صادره برای نقش A گنجانده می‌شود.	در محدوده قرارداد نیست
مجازشماری Authorization	۴۶. نقش‌ها (Roles) به دو سطح Realm-Level و Client-Level تقسیم می‌شوند و ساختار ارائه آن‌ها در توکن دسترسی به صورت realm_access.roles و resource_access.<client-id>.roles است.	در محدوده قرارداد نیست
مجازشماری Authorization	۴۷. ارث بری نقش ها در گروه امکان پذیر است و به زیر گروه‌ها انتقال پیدا می‌کند. برای مثال اگر نقش read_reports به گروه /دپارتمان/مالی اختصاص داده شود، تمام کاربران عضو این گروه و تمام زیرگروه‌های آن (مانند حسابداری) به‌صورت خودکار این نقش را دریافت می‌کنند.	در محدوده قرارداد نیست
مجوز دسترسی‌ها (Permissions)	۴۸. قابلیت مجوز دسترسی‌ها برای کلاینت‌های Confidential (سامانه‌های تخصصی) در SSO پلاس فعال است.	در محدوده قرارداد نیست

	۴۹. راهبر سامانه امکان تعریف Resource و Scope برای همه کلاینت‌های Confidential را در سامانه SSO پلاس دارد. ۵۰. امکان انتساب Resource/Scope به نقش وجود دارد. ۵۱. لیست مجوزهای دسترسی در Permission Token ارائه می گردد.	
مدیریت کلاینت‌ها	۵۲. سامانه امکان تنظیم کلاینت دارد و شامل امکان فعال و غیر فعال سازی کلاینت، محدود سازی برای Implicit Flow از استاندارد OAuth و ریست کردن Client_Secret و تنظیمات مرتبط با پروتکل ها توسط کاربر راهبر یا کاربر دارای نقش مدیریت کلاینت‌ها است. ۵۳. تمامی کاربران، می‌توانند از منوی پنجره سامانه‌ها، لیست کلاینت‌ها (سامانه‌های تخصصی) مجاز را مشاهده نمایند. دسته بندی و ترتیب نمایش کلاینت‌ها در این منو توسط راهبر اصلی سامانه قابل تنظیم است.	در محدوده قرارداد است
مدیریت گذرواژه (رمز عبور) و تعداد نشست مجاز	۵۴. امکان مدیریت سختی رمز عبور برای زمانی که رمزهای عبور در سامانه SSO پلاس نگهداری می‌شود و فرآیند احراز هویت هم بر اساس رمز عبور است توسط راهبر امکان پذیر است. ۵۵. راهبر امکان ریست کردن یا اجبار کاربر به تنظیم مجدد رمز عبور در لاگین بعدی را دارد. ۵۶. امکان تنظیم تعداد نشست مجاز توسط راهبر، برای همه کاربران با رعایت جلوگیری از ورود کاربران با یک شناسه بیش از تعداد نشست تنظیم شده.	فقط مدیریت تعداد نشست ها در محدوده قرارداد است
ماژول قوانین دسترسی Access Rule Engine	۵۷. ماژول قوانین دسترسی، امکان محدود سازی و متنوع سازی فرآیندهای احراز هویت (لاگین) به SSOپلاس را فراهم می کند و قابلیت‌های آن به شرح موارد مذکور است، این قابلیت مستقل از پروتکل OAuth/OIDC/SAML یا ورود به کلاینت‌ها است و مختص لاگین	در محدوده قرارداد نیست

	اصلی کاربر به SSOپلاس است. کارکرد این ماژول به این صورت است که در صورت فعال بودن، به محض ورود کاربر قوانین تعریف شده بررسی می‌گردد و اولین قانونی که با کاربر تطابق (Match) شود اعمال می‌گردد.	
ماژول قوانین دسترسی Access Rule Engine	۵۸. مدیریت این ماژول توسط کاربر راهبر SSOپلاس امکان پذیر است.	در محدوده قرارداد نیست
ماژول قوانین دسترسی Access Rule Engine	۵۹. فعال و غیر فعال سازی کامل ماژول امکان پذیر است.	در محدوده قرارداد نیست
ماژول قوانین دسترسی Access Rule Engine	۶۰. امکان تعیین سیاست پیش فرض Permit یا Deny در صورت عدم تطابق هیچ قانونی با کاربر در حال لاگین.	در محدوده قرارداد نیست
ماژول قوانین دسترسی Access Rule Engine	۶۱. امکان تعریف قانون با مشخصات: مخاطب (کاربر، گروه، نقش) و شرایط شامل (IP/CIDR، روزهای کاری، ساعات کاری، نوع کلاینت مثل تبلت/موبایل/دسکتاپ) است. ۶۲. بر اساس قانون تطبیق شده: امکان تعریف Permit/Deny وجود دارد. ۶۳. بر اساس قانون تطبیق شده راهبر می‌تواند فرآیند احراز هویت را از گزینه‌های موجود تنظیم نماید.	در محدوده قرارداد نیست
گزارش ها و سوابق	۶۴. سامانه امکان ثبت و مشاهده رویدادهای مرتبط با احراز هویت کاربران از جمله ورود موفق (Login Success) و ورود ناموفق (Login Failure) را در پنل مدیریتی فراهم می‌نماید.	در محدوده قرارداد است

	۶۵. سامانه امکان مشاهده و گزارش داخلی دارد، دسترسی استاندارد (DBView/syslog) برای برداشت لاگ وجود دارد، مسئولیت جمع‌آوری و تحلیل بیرونی با کارفرماست. ۶۶. استفاده از ابزارهای جمع‌آوری لاگ بیرونی از سطح سیستم‌عامل و پایگاه‌داده توسط کارفرما، از طریق مکانیزم‌های استاندارد زیرساختی در سطح سیستم‌عامل و پایگاه‌داده‌های SSOپلاس امکان‌پذیر است. ۶۷. گزارش‌ها و داشبوردهای داخلی بر رویدادهای مرتبط با SSO (ورود، خطای احراز هویت، تغییرات مدیریتی) و شاخص‌های سامانه متمرکز است. ۶۸. نگهداری لاگ‌های SSO در پنل مدیریتی بر اساس اعلام زمان درخواستی کارفرما در مرحله پیکربندی، تنظیم خواهد شد به صورت پیشرفت سه ماه در نظر گرفته شده است.	
تنظیمات پیشرفته	۶۹. راهبر اصلی سامانه می‌تواند تنظیمات IdP مثل دولت من را از طریق تنظیمات پیشرفته: تنظیمات IdP مدیریت نماید.	در محدوده قرارداد است
تنظیمات پیشرفته	۷۰. قابلیت تنظیم Token Mapper بر اساس خصیصه کاربران به claim های AccessToken و IDToken. ۷۱. قابلیت تنظیم Token Mapper بر اساس مقدار ثابت (Hard-Code) به claim های AccessToken و IDToken به صورت یکپارچه برای همه کاربران.	در محدوده قرارداد نیست

پیوست شماره(۳) قرارداد
(توافق‌نامه سطح خدمات)

ماده ۱- کلیات و تعاریف

۱-۱- این توافق‌نامه به‌منظور تبیین سطح خدمات پشتیبانی، نگهداری و پاسخ‌گویی فنی سامانه مدیریت هویت و دسترسی SSO پلاس منعقد می‌گردد.

۱-۲- سامانه: منظور، سامانه SSO پلاس است و گاها با اسامی زیر نیز شناخته می شود:

- Single Sign-On
- Identity Provider
- Authorization Server
- Identity Management

۱-۳- **خدمات پشتیبانی**: شامل مجموعه اقداماتی است که به‌منظور حفظ تداوم بهره‌برداری، رفع اشکالات و ارائه راهنمایی فنی مطابق این SLA ارائه می‌شود.

۱-٤- **محیط بهره‌برداری**: شامل زیرساخت سخت‌افزاری، نرم‌افزاری، شبکه، ارتباطات و سرویس‌های جانبی است که حسب مورد در اختیار یا تحت مسئولیت کارفرما یا اشخاص ثالث قرار دارد.

۱-۵- **ساعات ارائه خدمات پشتیبانی:** مطابق قرارداد اصلی تعیین و مبنای محاسبه تعهدات این SLA خواهد بود.

۱-٦- **سامانه‌های متصل**: به سامانه‌های مقصد اطلاق می‌شود که با SSO پلاس یکپارچه‌سازی کرده‌اند و امکان ورود کاربران به آن‌ها از طریق SSO پلاس فراهم شده است.

ماده ۲- دامنه خدمات مشمول SLA

۲-۱- خدمات موضوع این SLA ناظر بر موارد زیر است:

- پشتیبانی فنی سامانه در محدوده قابلیت‌ها و مشخصات نسخه تحویل‌شده مطابق با پیوست فنی
- بررسی رخدادهای مرتبط با فرآیند ورود کاربران به SSO پلاس

- ارائه اصلاحات و به‌روزرسانی‌های موردی مرتبط با نسخه مورد بهره‌برداری
- ارائه راهنمایی و مشاوره فنی در خصوص تنظیمات متعارف سامانه

۲-۲- خدمات زیر خارج از شمول این SLA بوده و در صورت امکان‌پذیری، مستلزم انعقاد قرارداد یا موافقت‌نامه جداگانه خواهد بود:

- توسعه قابلیت‌های جدید یا تغییر در منطق‌های کسب‌وکار در محدوده پیوست فنی قرارداد
- پشتیبانی از نرم‌افزارها، سخت‌افزارها و خدمات اشخاص ثالث
- رفع اشکالات ناشی از زیرساخت، شبکه، اینترنت، DNS، گواهی‌ها، فایروال، یا تغییرات اعمال شده بدون هماهنگی با فروشنده
- مشکلات ناشی از اطلاعات نادرست کاربران یا سیاست‌های داخلی کارفرما

ماده ۳- سطوح رخداد و معیار تشخیص اختلال در سامانه SSO پلاس

به‌منظور شفاف‌سازی مسئولیت‌ها و جلوگیری از اختلاف برداشت، سطوح رخداد در سامانه SSO پلاس **بر اساس اثر عملی آن بر کاربران و نتیجه ورود به سامانه‌های متصل** به شرح زیر تعریف می‌گردد:

۳-۱- اصل تشخیص سلامت سامانه SSO پلاس: چنانچه کاربر:

۱. بتواند وارد سامانه SSO پلاس شود

۲. و پس از ورود، حداقل به یکی از سامانه‌های متصل با موفقیت وارد گردد

سامانه SSO پلاس از منظر احراز هویت و صدور دسترسی سالم و فعال تلقی می‌گردد و مشکلات ورود به سایر سامانه‌ها مستقل از عملکرد SSO Plus خواهد بود، مگر آنکه خلاف آن به‌صورت مستند اثبات گردد.

۳-۲- سطح (۱) – بحرانی

رخدادهایی که باعث می‌شود بخش عمده کاربران سازمان عملاً نتوانند از طریق SSO پلاس وارد سامانه‌های خود شوند و انجام کارهای روزمره سازمان مختل گردد.

مصداق‌های روشن و قابل درک:

- کاربران از طریق اینترنت‌های مختلف سامانه SSO پلاس را نمی‌بینند
- کاربران نمی‌توانند وارد SSO Plus شوند (حتی با نام کاربری/رمز صحیح)
- ورود به SSO Plus انجام می‌شود اما برای هیچ‌کس هیچ سامانه‌ای باز نمی‌شود
- ادمین سامانه SSO پلاس نیز امکان ورود برای بررسی یا مدیریت را ندارد

به زبان ساده: «اکثر کاربران پشت در ورود مانده‌اند و هیچ سامانه‌ای باز نمی‌شود.»

تبصره ۱ :

موارد زیر، حتی در صورت بروز مشکل برای کاربران، به‌تنهایی نشانه اختلال در SSO پلاس نیست:

- عدم دسترس‌پذیری، کندی یا تغییر در "سامانه‌های متصل"
- تغییرات اعمال‌شده در "سامانه‌های متصل" بدون هماهنگی قبلی
- اختلال اینترنت، شبکه، DNS یا گواهی امنیتی
- خطاهای ناشی از اطلاعات نادرست کاربران

تبصره ۲ :

تشخیص نهایی سطح رخداد و منشأ آن، با لحاظ اثر واقعی بر کاربران و مستندات فنی، توسط فروشنده انجام می‌پذیرد.

۳-۳- سطح (۲) – بالا

رخدادهایی که موجب اختلال قابل توجه می‌شود اما کل سرویس متوقف نیست.

مصداق‌های روشن و قابل درک:

- ورود انجام می‌شود اما بسیار کند و ناپایدار است (گاهی موفق، گاهی ناموفق)
- کاربر وارد می‌شود اما به منوهایی که قبلاً دسترسی داشته، دسترسی ندارد

تبصره ۳ :

تا زمانی که ورود به SSO پلاس و ورود به حداقل یک سامانه متصل با موفقیت انجام شود، منشأ اختلال سامانه SSO پلاس تلقی نمی گردد مگر با ارائه شواهد فنی معتبر مبنی بر خلاف آن.

به زبان ساده: «اگر حداقل یک سامانه باز می‌شود، SSO پلاس سالم است و مشکل از "سامانه‌های متصل" یا زیرساخت آن‌هاست.»

۳-٤- سطح (۳) – متوسط

رخدادهایی که اثر مستقیم بر ورود کاربران ندارد و کار اصلی قابل انجام است، ولی کیفیت یا برخی امکانات کاهش یافته است.

مصداق‌های روشن و قابل درک:

- دسترسی کاربر توسط ادمین سامانه تغییر داده شده اما هنوز برای کاربر اعمال نشده
- گزارش‌ها یا آمارهای مدیریتی درست نمایش داده نمی‌شود
- پنل مدیریتی کند است یا بخشی از آن درست نمایش داده نمی‌شود

۳-۵- سطح (۴) – پایین

مواردی که اختلال عملیاتی محسوب نمی‌شوند و جنبه راهنمایی/بررسی/تغییرات جزئی دارند.

مصداق‌های روشن و قابل درک:

- درخواست اتصال یک سامانه جدید به SSO پلاس
- درخواست بررسی لاگ‌ها

- فعال/غیرفعال کردن یک تنظیم
- درخواست گزارش یا توضیح فنی

ماده ۴- زمان‌های هدف پاسخ‌گویی

زمان‌ها هدف بوده و مشروط به همکاری کارفرما و فراهم بودن دسترسی‌های لازم است

سطح رخداد	پاسخ
سطح ۱	۴ ساعت
سطح ۲	۲۴ ساعت
سطح ۳	۳ روز کاری
سطح ۴	۱۰ روز کاری

ماده ۵- سطح دسترس‌پذیری سامانه SSO پلاس

۵-۱- **تعریف:** سطح دسترس‌پذیری SSO پلاس به معنای **امکان ورود موفق کاربران به SSO پلاس و دسترسی به حداقل یکی از سامانه‌های متصل** در بازه زمانی مورد نظر است.

۵-۲- **سطح دسترس‌پذیری هدف:** سطح دسترس‌پذیری هدف با توجه به نوع دسترسی به محیط عملیاتی خریدار به میزان ۹۹٪ می‌باشد.

۵-۳- **روش محاسبه:** (۱۰۰× کل زمان ماه) ÷ (زمان اختلال معتبر – کل زمان ماه) = سطح دسترس‌پذیری سامانه

۵-٤- **اختلال معتبر:** اختلال معتبر حالتی است که کاربران قادر به ورود به SSO پلاس نباشند یا پس از ورود، هیچ یک از سامانه‌های متصل امکان ورود کاربر را نداشته باشد و به صورت مستند ریشه مشکل SSO پلاس تشخیص داده شود.

۵-۵- موارد مستثنی از محاسبه:

- نگهداری برنامه‌ریزی شده با هماهنگی خریدار
- اختلال زیرساخت / شبکه / اینترنت / DNS/ گواهی‌ها
- اختلال سامانه‌های متصل یا سرویس‌های ثالث
- تغییرات بدون هماهنگی
- شرایط فورس ماژور
- مواردی که ورود به SSO پلاس و حداقل یک سامانه متصل موفق باشد

۵-۶- **مرجع تشخیص:** مرجع تشخیص و اندازه‌گیری، لاگ‌ها و ابزارهای پایش می‌بایست مورد تایید فروشنده باشد.

۵-۷- **جبران عدم تحقق:** جبران صرفاً در قالب **اعتبار خدمات پشتیبانی آتی** و حداکثر تا سقف **10٪ مبلغ خدمات پشتیبانی همان دوره** انجام می‌گردد و قابل تبدیل به وجه نقد یا انتقال به غیر نیست.

ماده ۶- حدود مسئولیت

مسئولیت فروشنده در هر حال از مجموع مبالغ دریافتی بابت خدمات پشتیبانی در دوره مربوطه تجاوز نخواهد کرد و فروشنده در قبال خسارات غیرمستقیم (از جمله از دست رفتن سود، وقفه کسب‌وکار و ادعاهای اشخاص ثالث) مسئولیتی ندارد.

ضمیمه – A چک‌لیست تشخیص مشکل قبل از تماس با پشتیبانی SSO پلاس

قبل از تماس با پشتیبانی، این ۶ سؤال را پاسخ دهید:

۱. آیا SSO پلاس از طریق اینترنت‌های مختلف قابل مشاهده است؟ ☐ بله ☐ خیر

۲. آیا می‌توانید وارد SSO Plus شوید؟ ☐ بله ☐ خیر

۳. آیا بعد از ورود، حداقل یک سامانه متصل برای شما باز می‌شود؟ ☐ بله ☐ خیر

٤. آیا مشکل فقط مربوط به یک سامانه خاص است؟ ☐ بله ☐ خیر

٥. آیا اخیراً در آن سامانه (یا زیرساخت آن) تغییری انجام شده است؟ ☐ بله ☐ خیر/اطلاع ندارم

٦. آیا سایر کاربران هم همین مشکل را دارند؟ ☐ بله ☐ خیر

راهنمای سریع تصمیم‌گیری:

- اگر (۱=خیر و ۲=خیر) ← احتمال اختلال در SSO پلاس وجود دارد ← با پشتیبانی تماس بگیرید.
- اگر (۱=بله و ۲=بله و ۳=بله) ← احتمالاً SSO Plus سالم است ← ابتدا سامانه مقصد/زیرساخت بررسی شود.
- اگر (۴=بله) ← مشکل غالباً مربوط به همان سامانه مقصد است.