به نام خدا

سند هدف امنیتی سامانه جامع IGS- نسخه۳.۴.۰.۲

سامانه های سبز هوشمند

فروردین-۱۴۰۰

نسخه **۱.۲**

فهرست

۱ مقدمه

این پروفایل حفاظتی، به بیان الزامات برنامه کاربردی می‌پردازد. این سند بر اساس سند طرح ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 تهیه گردیده است.

۲ اصطلاحات

استاندارد ارزیابی معیار مشترک (CC): استاندارد ارزیابی معیار مشترک برای ارزیابی امنیت فناوری‌های اطلاعات.

متدلوژی ارزیابی معیار مشترک[1] (CEM): متدلوژی ارزیابی معیار مشترک برای ارزیابی امنیت فناوری‌های اطلاعات.

محصول (TOE): محصول مورد ارزیابی؛ که در این سند، نرم‌افزار کاربردی و مستندات پشتیبان آن است.

غیر محصول (Non-TOE[2]): سخت‌افزار، نرم‌افزار و میان‌افزاری که محصول جهت اجرا به آن‌ها نیز نیاز دارد.

محیط عملیاتی (Operational Environment): محیطی که محصول در آن عمل می‌کند.

پروفایل حفاظتی (PP[3]): مجموعه‌ای از الزامات امنیتی برای دسته‌ای از محصولات؛ مجموعه‌ای که مستقل از پیاده‌سازی است.

هدف امنیتی (ST[4]): مجموعه‌ای از الزامات امنیتی برای یک محصول خاص؛ مجموعه‌ای که وابسته به پیاده‌سازی است.

بسته (Package): نام مجموعه‌ای از الزامات کارکرد امنیتی یا تضمین امنیتی می‌باشد. به عنوان مثال EAL3.

سطح تضمین ارزیابی(EAL[5]): مجموعه‌ای از الزامات تضمین که از قسمت سوم از سندهای سه‌گانه «استاندارد ارزیابی معیار مشترک» برگرفته شده است، و نشان دهنده سطح امنیتی محصول می‌باشد. سطوح تضمین از سطح ۱ تا سطح ۷ می‌باشند، لازم به ذکر است که «سطح تضمین امنیتی» یک نوع «بسته» می‌باشد.

خلاصه مشخصه محصول[6] (TSS): شرحی از این‌که یک محصول چگونه الزامات کارکرد امنیتی را در یک هدف امنیتی برآورده می‌سازد.

داده کاربری (User data): داده‌های کاربری هستند که کارکرد امنیتی محصول را تحت تأثیر قرار نمی‌دهند. این داده‌ها اطلاعاتی ذخیره شده در منابع محصول هستند که توسط کاربران مطابق با الزامات کارکرد امنیتی به کار برده می‌شود. محتویات یک پیام الکترونیک نوعی داده کاربری می‌باشد.

سرپرست (Administrator): موجودیتی که مسئولیت مدیریت و اعمال خط‌مشی‌ها را بر روی محصول بر عهده دارد و معمولاً دارای بالاترین سطح مجوز است.

موجودیت فعال (Subject): موجودیت فعال، موجودیتی در سیستم مورد ارزیابی (محصول) است که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون سرپرست، کاربر نهایی و غیره. به عبارت دیگر موجودیت فعال عامل انجام عملی بر روی محصول است.

---

[1] Common Evaluation Methodology(CEM)
[2] Non-Target Of Evaluation
[3] Protection Profile
[4] Security Target
[5] Evaluation Assurance Level
[6] TOE Summary Specification (TSS)

موجودیت غیرفعال (Object): موجودیت غیرفعال، موجودیتی در سیستم مورد ارزیابی (محصول) می‌باشد که شامل اطلاعات است و یا اطلاعات را دریافت می‌نماید، و روی آن توسط موجودیت‌های فعال، عملیاتی انجام می‌گیرد. همانند داده‌ها و اطلاعاتی همچون متن‌های رمز شده و کلیدها و غیره. به عبارت دیگر موجودیتی است که توسط موجودیت فعال بر روی آن رخدادی اتفاق می‌افتد، مانند لیست کردن رکوردها توسط سرپرست، حذف فایل‌ها توسط حمله کننده، که در این دو مثال رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.

راز (Secret): اطلاعاتی که باید تنها به کاربران مجاز و/یا محصول شناسانده شود، تا یک «خط‌مشی کارکرد امنیتی » اجرا گردد.

مشخصه امنیتی(Security attribute): کاربران، موجودیت‌های فعال، اطلاعات، موجودیت‌های غیرفعال، نشست‌ها و منابع تحت کنترل قوانین «الزامات کارکرد امنیتی» ممکن است دارای اطلاعات خاصی باشند که جهت کارکرد صحیح محصول، مورد استفاده قرار گیرند. دسته‌ای از این اطلاعات حالت آگاهی‌دهنده دارند همچون نام فایل که ممکن است برای معرفی منابع منحصر به فرد استفاده شود، اما دسته‌ی دیگر از این اطلاعات ممکن است به طور خاص برای اجرا شدن الزامات کارکرد امنیتی وجود داشته باشند، همانند اطلاعات کنترل دسترسی، این دسته از اطلاعات به طور کلی «مشخصه امنیتی» نامیده می‌شود.

خط‌مشی کارکرد امنیتی(SFP[7]): رفتار امنیتی که توسط «کارکرد امنیتی محصول» اجرا می‌گردد تحت مجموعه قوانینی در «الزامات کارکرد امنیتی» بیان می‌شوند، این مجموعه قوانین «خط‌مشی کارکرد امنیتی» نامیده می‌شوند. «الزامات کارکرد امنیتی» ممکن است چندین خط‌مشی جهت معرفی قوانینی که محصول باید اجرا نماید، تعریف کند. هر کدام از خط‌مشی‌ها باید حوزه کنترلی‌اش را توسط موجودیت‌های فعال، موجودیت‌های غیرفعال، منابع یا اطلاعات و عملکردهایی که بکار برده است، مشخص نماید. تمام این خط‌مشی‌ها توسط «محصول» پیاده‌سازی می‌شوند.

خط‌مشی کارکرد امنیتی کنترل دسترسی (Access control SFP): چندین خط‌مشی کارکرد امنیتی وجود دارد که برای حفاظت از داده‌ها بکار برده می‌شوند، همچون «خط‌مشی کنترل دسترسی» و «خط‌مشی کنترل جریان اطلاعات». «خط‌مشی کنترل دسترسی» مکانیزم‌هایی هستند که براساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی کاربران، منابع، موجودیت‌های فعال، موجودیت‌های غیرفعال، نشست‌ها، TSF status data و عملکردها در حوزه کنترلی‌شان پیاده‌سازی می‌شوند.

این مشخصه‌های امنیتی در مجموعه قوانینی استفاده می‌شوند که حاکم بر عملیاتی است که موجودیت‌های فعال ممکن است بر روی موجودیت‌های غیرفعال اجرا نمایند.

خط‌مشی کنترل جریان اطلاعات (Information Flow Control SFP): «خط‌مشی جریان اطلاعات» مکانیزم‌هایی هستند که براساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی موجودیت‌های فعال و اطلاعات در حوزه کنترلی‌شان و مجموعه قوانین حاکم بر عملیات که توسط موجودیت فعال بر روی اطلاعات صورت می‌گیرد، پیاده‌سازی می‌شوند.

[7] Security Functionality Policy

تصادفی‌سازی نمایه فضای آدرس[8] (ASLR): یک قابلیت ضد اکسپلویت که نگاشت حافظه را در مکان‌های غیرقابل پیش‌بینی انجام می‌دهد. ASLR، کار مهاجمان را برای به دست گرفتن کنترل دستگاه از طریق کدی که وارد فضای آدرس برنامه کاربردی کرده‌اند، دشوارتر می‌نماید.

برنامه کاربردی[9] (App): نرم‌افزاری که به همراه واسط برنامه‌نویسی برنامه کاربردی (API)، روی یک پلتفرم اجرا می‌شود و از جانب کاربر یا مالک پلتفرم وظایفی را انجام می‌دهد. در این سند می‌توان دو اصطلاح محصول و برنامه کاربردی را به جای یکدیگر به کار برد.

واسط برنامه‌نویسی برنامه کاربردی[10] (API): مجموعه‌ی معینی از روش‌ها، ساختارهای داده، رده‌بندی اشیا، و متغیرهایی که به یک برنامه کاربردی اجازه می‌دهند تا از سرویس‌هایی که توسط مؤلفه نرم‌افزاری دیگری فراهم شده است، مانند یک کتابخانه، استفاده کند. APIها اغلب برای مجموعه‌ای از کتابخانه‌هایی که در یک پلتفرم وجود دارد، ایجاد می‌شوند.

اعتبارنامه[11]: داده‌های حساب کاربری که هویت کاربر را شکل می‌دهند، مانند گذرواژه‌ها و کلیدهای رمزنگاری.

جلوگیری از اجرای داده‌ها[12] (DEP): یک قابلیت ضد اکسپلویت در سیستم‌عامل‌های مدرن که روی سخت‌افزارهای کامپیوتری مدرن اجرا می‌شود و اجرای دستورات را در برخی از صفحات حافظه غیرممکن می‌سازد. قابلیت جلوگیری از داده‌ها به صفحات حافظه اجازه نمی‌دهد که حاوی داده‌ها و هم دستورالعمل‌ها باشند. در این صورت، کار مهاجمان برای تزریق و اجرای کد، سخت‌تر می‌شود.

تولید کننده [13]: نهادی که نرم‌افزار برنامه‌های کاربردی را می‌نویسد. در این سند، فروشنده و تولیدکننده در یک معنا به کار می‌روند.

کد موبایل: نرم‌افزاری که از یک سیستم راه دور برای اجرا درون یک محیط اجرایی محدود روی سیستم‌های محلی، ارسال می‌شود. عموماً این کدها به صورت دائمی نصب نمی‌شوند و اجرای آن‌ها بدون اطلاع کاربر یا حتی هشدار آغاز می‌شود. مثال‌هایی از فناوری‌های کد موبایل عبارتند از: جاوا اسکریپت، جاوا اپلت‌ها، Adobe Flash و Microsoft Silverlight.

سیستم‌عامل (OS): نرم‌افزاری که منابع سخت‌افزاری را مدیریت می‌کنند و برای برنامه‌های کاربردی، خدمات فراهم می‌کند.

اطلاعات شناسایی شخصی[14] (PII): هرگونه اطلاعات در مورد یک فرد که توسط یک سازمان نگهداری می‌شود؛ اطلاعاتی مانند سوابق تحصیلی، تراکنش‌های مالی، سابقه پزشکی، سابقه کیفری یا سابقه استخدامی و هرگونه اطلاعاتی که بتوان از آن‌ها هویت یک فرد را تشخیص داد یا رهگیری کرد؛ مانند نام، شماره تأمین اجتماعی، تاریخ و محل تولد، نام خانوادگی مادر قبل از ازدواج، اطلاعات جسمی و هرگونه اطلاعات شخصی دیگری که مرتبط با فرد باشد یا بتوان از طریق آن به فرد ارتباطی پیدا کرد.

---

[8] Address Space Layout Randomization
[9] Application
[10] Application Programming Interface
[11] Credential
[12] Data Execution Prevention
[13] Developer
[14] Personally Identifiable Information

پلتفرم: محیطی که نرم‌افزار برنامه کاربردی در آن اجرا می‌شود. پلتفرم می‌تواند یک سیستم‌عامل باشد، یک محیط اجرایی باشد که روی سیستم‌عامل کار می‌کند، یا ترکیبی از این حالت‌ها باشد.

داده‌های حساس: داده‌های حساس ممکن است شامل تمامی داده‌های شخصی یا سازمانی شود و یا بخش خاصی از داده‌های برنامه‌های کاربردی مثل ایمیل، پیام‌ها، سندها، اطلاعات تقویم، و تماس‌ها را در بر گیرد. برای این که داده‌ای، حساس محسوب شود باید حداقل حاوی اطلاعات شناسایی شخصی، اطلاعات حساب کاربری یا کلیدها باشد. داده‌های حساس در خلاصه مشخصه محصول برنامه کاربردی و توسط فردی که هدف امنیتی را تعیین می‌کند، شناسایی می‌شوند.

کوکی پشته[15] : یک قابلیت ضد اکسپلویت که ابتدای فراخوانی تابع، یک مقدارِ عددی را به آن نسبت می‌دهد و در پایان فراخوانی تابع بررسی می‌کند که آیا این مقدار عددی تغییر کرده است یا خیر. به این کار محافظ پشته[16] یا قناری‌های پشته[17] نیز می‌گویند.

فروشنده: نهادی که نرم‌افزار برنامه کاربردی را می‌فروشد. در این سند، دو اصطلاح تولیدکننده و فروشنده، معادل با یکدیگرند. فروشندگان مسئول نگهداری و به‌روزرسانی نرم‌افزار برنامه کاربردی خود هستند.

انتخاب: «اانتخاب» یکی از عملیات‌هایی است که در الزامات پروفایل جهت منعطف شدن پروفایل به منظور تدوین سند هدف امنیتی توسط تولید کننده آمده است. در الزاماتی با این عملیات نویسنده با توجه به کارکرد امنیتی محصول یک یا چند مورد از موارد ذکر شده در الزام را انتخاب می‌نماید و به عنوان ادعا در بخش الزامات کارکردی سند هدف امنیتی ذکر می‌نماید.

اختصاص: «اختصاص» یکی از عملیات‌هایی است که در الزامات پروفایل جهت منعطف شدن پروفایل به منظور تدوین سند هدف امنیتی توسط تولید کننده آمده است. در الزاماتی با این عملیات نویسنده با توجه به کارکرد امنیتی محصول، مقدار یا پارامتر مشخصی را اختصاص می‌دهد.

۳ شرح محصول

نرم افزار سامانه جامعIGS تحت شبکه بوده و شامل زیرسیستم های: دبیرخانه، فرم ساز، حسابداری و حقوق دستمزد می باشد و عناصر سخت افزاری و نرم افزاری آن به شرح زیر می باشد:

حوزه فیزیکی

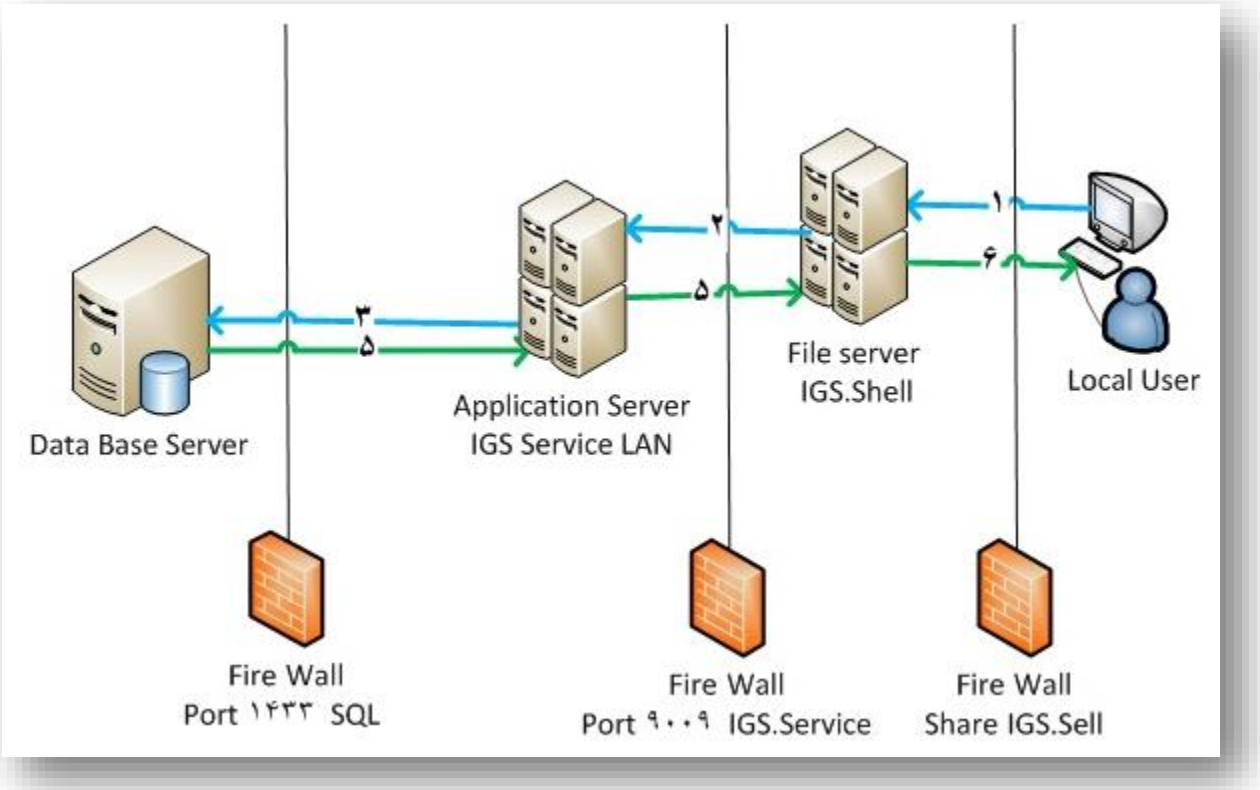
عناصر سخت‌افزاری و نرم‌افزاری مورد استفاده با توجه به پیکربندی ارزیابی در جدول زیر معرفی می‌شود:

عناصر هدف ارزیابی	شماره مدل یا نسخه
سیستم‌عامل سرور	Win 2008R2
Ram سرور	4GB
HDD سرور	50GB

[15] Stack Cookie
[16] Stack Guard
[17] Stack Canaries

CPU سرور	Core I 5
سیستم‌عامل کلاینت	Win XP SP3/ Win 7 SP1
کارت شبکه	حداقل Onboard
پایگاه داده سرور	SQL2019
مرورگر کلاینت	ندارد
وب سرور	ندارد
زبان برنامه‌نویسی	C# .NET
سایر نرم‌افزارهای کلاینت	۱. MS Office 2003/2007 ... ۲. Adobe Acrobat Reader 6+ ۳. MS ImagingProfessional V 2.5 + .Net FrameWork4.0
سایر نرم‌افزارهای سرور	.Net FrameWork4.0

پیکربندی و قرارگیری هدف ارزیابی در محیط عملیاتی : (شمای ارتباطات و اجزا محصول)



مورد استفاده ۱: ایجاد محتوا

برنامه کاربردی به کاربر اجازه می‌دهد تا تولید محتوا کند و آن را در فضای حافظه محلی یا از راه دور، ذخیره نماید. برخی از نمونه‌های این محتوا عبارتند از: سند متنی، اسلاید و تصویر.

مورد استفاده ۲: مصرف محتوا

برنامه کاربردی به کاربر اجازه می‌دهد تا محتوا را از فضای حافظه‌ی محلی یا از راه دور به دست آورده و بکار برد. برخی از نمونه‌های این محتوا عبارتند از: ویدئو و صفحات وب.

مورد استفاده ۳: ارتباطات

برنامه کاربردی به کاربر اجازه می‌دهد تا از طریق یک کانال ارتباطی، به صورت تعاملی یا غیرتعاملی با دیگر کاربران یا برنامه‌های کاربردی ارتباط برقرار کند. نمونه‌هایی از ارتباطات عبارتند از: پیام فوری، ایمیل و ارتباط صوتی.

۴ مسائل امنیتی

مسائل امنیتی یعنی تهدیداتی که از محصول انتظار می‌رود آنان را رفع کند، فرضیاتی که در مورد محیط عملیاتی وجود دارد، و هرگونه سیاست امنیتی سازمانی که از محصول برای اجرای آن استفاده می‌شود.

۴,۱ تهدیدات

تهدیدات	توضیحات
T.NETWORK_ATTACK	فرد مهاجم روی یک کانال ارتباطی یا هر جای دیگری از زیرساخت شبکه قرار می‌گیرد. مهاجمان ممکن است سعی در برقراری ارتباط با برنامه کاربردی نمایند یا در ارتباطات میان نرم‌افزار برنامه کاربردی و دیگر نقاط پایانی دست ببرند تا بتوانند به آن نفوذ کنند.
T.NETWORK_EAVESDROP	فرد مهاجم روی یک کانال ارتباطی یا هر جای دیگری از زیرساخت شبکه قرار می‌گیرد. مهاجمان ممکن است داده‌های انتقالی بین برنامه کاربردی و دیگر نقاط پایانی را مشاهده کنند یا به آن‌ها دسترسی یابند.
T.LOCAL_ATTACK	فرد مهاجم ممکن است از طریق نرم‌افزارهای عادی (نرم‌افزارهایی که امتیاز دسترسی ویژه ندارند) موجود روی پلتفرمی که برنامه کاربردی روی آن اجرا می‌شود، وارد عمل شود. مهاجمان ممکن است ورودی‌های آلوده را در قالب فایل یا ارتباطات محلی، وارد برنامه کاربردی کنند.
T.PHYSICAL_ACCESS	مهاجم ممکن است به اطلاعات حساس بایگانی‌شده، دسترسی پیدا کند.

۴,۲ فرضیات

A.TYPES	توضیحات
A.PLATFORM	اجرای محصول منوط به یک پلتفرم رایانشی قابل اعتماد است و شامل پلتفرم زیرین و هرگونه محیط زمان اجرا که پلت فرم برای محصول فراهم کرده است، می‌باشد.
A.PROPER_USER	کاربر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، به کار می‌گیرد.
A.PROPER_ADMIN	راهبر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند، بی‌دقت نیست و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، راهبری می‌نماید.

۴,۳ خط‌مشی‌های امنیتی سازمانی

هیچ‌گونه خط‌مشی امنیتی سازمانی[18] برای برنامه کاربردی وجود ندارد.

۵ اهداف امنیتی

۵,۱ اهداف امنیتی برای محصول

هدف امنیتی	توضیحات
O.INTEGIRITY	محصولات انطباق‌پذیر، صحت نصب خود و بسته‌های به‌روزرسانی را تضمین می‌کنند و همچنین اقدامات اجرایی محیط محور را در جهت کاهش تهدیدات، تسهیل می‌نمایند. نرم‌افزارهای خیلی کمی، اگر نگوییم هیچ، عاری از خطا هستند. بنابراین، توانایی نصب بسته‌های تعمیر و عیب‌یابی و به‌روزرسانی نرم‌افزارهای نصب‌شده به صورت منسجم، اقدامی ضروری برای امنیت شبکه‌های سازمانی است. سازندگان پردازشگرها، برنامه‌نویسان کامپایلر، فروشندگان محیط‌های اجرا، و فروشندگان سیستم‌عامل‌ها، اقدامات اجرایی محیط محوری را در جهت کاهش تهدیدات ایجاد کرده‌اند که با پیچیده‌تر کردن وظایف سیستم‌ها، کار نفوذ به آن‌ها را برای مهاجمان، دشوارتر و پرهزینه‌تر می‌کند. نرم‌افزارهای برنامه کاربردی اغلب می‌توانند

[18] OSP

هدف امنیتی	توضیحات
	از این مکانیزم‌ها بهره ببرند. این کار با استفاده از APIهایی انجام می‌شود که در زمان اجرا فراهم شده است؛ یا توسط فعال‌سازی این مکانیزم‌ها از طریق کامپایلر یا لینکر.
O.QUALITY	برای تضمین کیفیت پیاده‌سازی، محصولات انطباق‌پذیر به جای پیاده‌سازی سرویس‌ها و APIهای خود، سرویس‌ها و APIهایی را به کار می‌گیرند که توسط محیط زمان اجرا تأمین شده است. اهمیت این کار به طور خاص برای سرویس‌های رمزنگاری و دیگر عملیات پیچیده‌ای مثل تجزیه فایل و رسانه، بیشتر است. بهره‌گیری از این قابلیت پلتفرم، فقط منوط به استفاده از APIهای مستند و پشتیبانی شده است.
O.MANAGEMENT	برای تسهیل روند مدیریت توسط کاربران و سازمان، محصولات انطباق‌پذیر، واسط‌های منسجم و پشتیبانی شده‌ای را برای نگهداری و پیکربندی امنیتی خود فراهم می‌کنند. این کار شامل پیاده‌سازی و به‌روزرسانی برنامه کاربردی با استفاده از قالب‌ها و مکانیزم‌های پیاده‌سازی پشتیبانی شده توسط پلتفرم و همچنین فراهم کردن مکانیزم‌هایی برای پیکربندی می‌باشد.
O.PROTECTED_STORAGE	برای جلوگیری از افشای اطلاعات محرمانه‌ی کاربر در نتیجه‌ی حوادثی که منجر به از دست رفتن کنترل فیزیکی ابزارهای ذخیره‌سازی می‌شوند، محصولات انطباق‌پذیر از شیوه‌های حفاظت داده‌های بایگانی‌شده استفاده می‌کنند. این کار شامل رمزگذاری داده‌ها و ذخیره کلیدها توسط محصول است تا از دسترسی غیرمجاز به این داده‌ها جلوگیری شود.
O.PROTECTED_COMMS	برای جلوگیری از حملات تهدیدآمیز فعال (دست‌کاری بسته‌های داده) و غیرفعال (استراق سمع)، محصولات انطباق‌پذیر از یک کانال مورد اعتماد برای انتقال داده‌های حساس استفاده می‌کنند. داده‌های حساس شامل کلیدهای رمزنگاری، گذرواژه‌ها، و هرگونه داده‌های دیگری است که مربوط به برنامه کاربردی بوده و نباید خارج از برنامه کاربردی، در معرض دید باشند.

۵,۲ اهداف امنیتی برای محیط عملیاتی

OE.TYPES	توضیحات
OE.PLATFORM	اجرای محصول متکی به یک پلتفرم رایانشی مورد اعتماد است. این شامل سیستم‌عامل زیرین و هرگونه محیط اجرایی دیگری نیز می‌شود که در اختیار محصول قرار گرفته است.
OE.PROPER_USER	کاربر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، به کار می‌گیرد.
OE.PROPER_ADMIN	راهبر برنامه کاربردی بی‌دقت نیست و از روی عمد دست به اشتباه یا خرابکاری نمی‌زند، و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، راهبری می‌نماید.

۶ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند. در ادامه هر یک از الزامات شرح و بسط داده شده‌اند.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۲	ذخیره‌سازی اسرار ۱	FCS_STO_EXT.1.1
۳	دسترسی به منابع پلتفرم ۱	FDP_DEC_EXT.1.1
٤	دسترسی به منابع پلتفرم ۲	FDP_DEC_EXT.1.2
٥	ارتباطات شبکه‌ای۱	FDP_NET_EXT.1.1
٦	رمزگذاری داده‌های حساس برنامه کاربردی ۱	FDP_DAR_EXT.1.1
۷	استفاده کاربر از یک سرویس بدون افشاء هویت ۴	FPR_ANO_EXT.1.1
۸	سازوکار پیکربندی پشتیبان‌شده ۱	FMT_MEC_EXT.1.1
۹	تأمین امنیت با پیکربندی پیش‌فرض۱	FMT_CFG_EXT.1.1
۱۰	تأمین امنیت با پیکربندی پیش‌فرض ۲	FMT_CFG_EXT.1.2
۱۱	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۱۲	استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱	FPT_API_EXT.1.1
۱۳	قابلیت‌های ضد اکسپلویت ۱	FPT_AEX_EXT.1.1
۱۴	قابلیت‌های ضد اکسپلویت ۲	FPT_AEX_EXT.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۵	قابلیت‌های ضد اکسپلویت ۳	FPT_AEX_EXT.1.3
۱۶	قابلیت‌های ضد اکسپلویت ۴	FPT_AEX_EXT.1.4
۱۷	قابلیت‌های ضد اکسپلویت ۵	FPT_AEX_EXT.1.5
۱۸	به‌روزرسانی امن۱	FPT_TUD_EXT.1.1
۱۹	به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۲۰	به‌روزرسانی امن ۳	FPT_TUD_EXT.1.3
۲۱	به‌روزرسانی امن ۴	FPT_TUD_EXT.1.4
۲۲	به‌روزرسانی امن ۵	FPT_TUD_EXT.1.5
۲۳	به‌روزرسانی امن ۶	FPT_TUD_EXT.1.6
۲۴	استفاده از کتابخانه‌های شخص ثالث ۱	FPT_LIB_EXT.1.1
۲۵	حفاظت از تبادل داده‌ها ۱	FTP_DIT_EXT.1.1
الزامات پیوست یک		
۲۶	پروتکل TLS Client (۱)	FCS_TLSC_EXT.1.4
الزامات پیوست دو		
۲۷	تولید بیت تصادفی ۳	FCS_RBG_EXT.2.1
۲۸	تولید بیت تصادفی ۴	FCS_RBG_EXT.2.۲
۲۹	مدیریت کلید رمزنگاری ۵	FCS_CKM_EXT.1.1
۳۰	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1
۳۱	مدیریت کلید رمزنگاری ۲	FCS_CKM.2.1
۳۲	عملیات رمزنگاری – رمزنگاری/رمزگشایی ۱ (۱)	FCS_COP.1.1(1)
۳۳	عملیات رمزنگاری – درهمسازی ۱ (۲)	FCS_COP.1.1(2)
۳۴	عملیات رمزنگاری – امضاء ۱ (۳)	FCS_COP.1.1(3)
۳۵	عملیات رمزنگاری – امضاء ۲ (۴)	FCS_COP.1.1(۴)
۳۶	پروتکل TLSC (۱)	FCS_TLSC_EXT.1.1
۳۷	پروتکل TLSC(۲)	FCS_TLSC_EXT.1.2
۳۸	پروتکل TLSC(۳)	FCS_TLSC_EXT.1.3
۳۹	پروتکل TLSC(۴)	FCS_TLSC_EXT.1.4
۴۰	پروتکل TLSS(۵)	FCS_TLSC_EXT.1.۵
۴۱	پروتکل DTLS (۱)	FCS_DTLS_EXT.1.1
۴۲	پروتکل DTLS (۲)	FCS_DTLS_EXT.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۴۳	پروتکل DTLS (۳)	FCS_DTLS_EXT.1.3
۴۴	پروتکل HTTPS (۱)	FCS_HTTPS_EXT.1.1
۴۵	پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2
۴۶	پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۴۷	الزامات پروتکل X509 (۱)	FIA_X509_EXT.1.1
۴۸	الزامات پروتکل X509 (2)	FIA_X509_EXT.1.2
۴۹	الزامات پروتکل X509 (3)	FIA_X509_EXT.2.1
۵۰	الزامات پروتکل X509 (4)	FIA_X509_EXT.2.2

۶/۱ کلاس ممیزی امنیت

شماره الزام	نام الزام
۱	**تولید بیت تصادفی ۱**
برنامه کاربردی برای عملیات رمزنگاری از هیچگونه عملکرد تولید بیت تصادفی قطعی استفاده نمی کند.	
۲	**ذخیره‌سازی اسرار ۱**
برنامه کاربردی در فضای حافظه غیر فرّار عملکردی برای ذخیره امن **فقط نام کاربرکه برای ورود مجدد ذخیره میکند** را پیاده‌سازی می کند. در مسیر زیر: Registry>CurrentUser>IGS>Shell با توجه به نحوه ورود تنظیم شده در مسیر: سیستم> تنظیمات سیستم> تب تنظیمات اصلی، که شناسه کاربری یا نام و نام خانوادگی باشد، اطلاعات بدون رمز در Registry نوشته می شود ولی رمز آنها جایی ذخیره نمی شود.	

۶,۲ کلاس حفاظت از داده‌ها

شماره الزام	نام الزام
۳	**دسترسی به منابع پلتفرم ۱**
برنامه کاربردی باید کاربر را از قصد خود برای دسترسی به این منابع، آگاه کند: • هیچگونه منبع سخت‌افزاری	
٤	**دسترسی به منابع پلتفرم ۲**
برنامه کاربردی باید کاربر را از قصد خود برای دسترسی به این منابع، آگاه کند: • هیچ نوع از منابع اطلاعات حساس	
٥	**ارتباطات شبکه‌ای۱**
برنامه کاربردی ارتباطات شبکه‌ای خود را محدود می کند به **برقراری ارتباط با IP با Port مشخص که در فایل Config توسط مدیر سیستم با نام Remote Server و Remote Port تنظیم شده است.**	
٦	**رمزگذاری داده‌های حساس برنامه کاربردی ۱**
برنامه کاربردی عملکردی برای رمزگذاری داده‌های حساس پیاده‌سازی می کند، داده های حساس با RSA و یک کلید عمومی رمز می شوند و اطلاعات بصورت رمز شده سمت سرور ارسال می شوند در سمت سرور با کلید خصوصی از رمز بیرون می آیند.	
۷	**استفاده کاربر از یک سرویس بدون افشاء هویت ۴**
برنامه کاربردی اطلاعات شناسایی شخصی(PII)را در شبکه انتقال نمی دهد. اطلاعاتی به جز نام کاربری و رمز عبور منتقل نمی شود که آن هم بصورت رمز شده است.	
۸	**سازوکار پیکربندی پشتیبان‌شده ۱**

شماره الزام	نام الزام
برنامه کاربردی سازوکار توصیه شده توسط تولیدکننده پلتفرم را برای ذخیره‌سازی و تنظیم گزینه‌های پیکربندی، استفاده می نماید.	
۹	**تأمین امنیت با پیکربندی پیش‌فرض۱**
هنگامی که برنامه کاربردی بدون اعتبارنامه یا با اعتبارنامه پیش‌فرض پیکربندی شده است، برنامه کاربردی اقدامات لازم برای ایجاد اعتبارنامه جدید را فراهم می آورد.	
۱۰	**تأمین امنیت با پیکربندی پیش‌فرض ۲**
برنامه کاربردی به طور پیش‌فرض طوری پیکربندی می شود که با قرار دادن مجوزهای دسترسی به فایل مناسب، خود برنامه کاربردی و داده‌های آن را از دسترسی‌های غیرمجاز محافظت می کند.	
۱۱	**کارکرد مدیریتی محصول ۱**
محصول باید قابلیت اجرای کارکردهای امنیتی زیر را داشته باشد: • **امکان قفل و باز کردن سیستم توسط مدیر سیستم، تعریف سطوح دسترسی هر نوع عملیات(ایجاد، حذف، ویرایش و نمایش)توسط مدیر سیستم**	

۶,۳ کلاس حفاظت از محصول

شماره الزام	نام الزام
۱۲	**استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱**
برنامه کاربردی تنها از واسط برنامه‌نویسی کاربردی‌های(API)پلتفرم پشتیبانی شده استفاده می کند.	
۱۳	**قابلیت‌های ضد اکسپلویت ۱**
برنامه کاربردی درخواست نگاشت حافظه به آدرس مشخصی می نماید.	
۱۴	**قابلیت‌های ضد اکسپلویت ۲**
برنامه کاربردی هیچ بخشی از حافظه را همزمان هم به نوشتن اطلاعات و هم اجرای مجوزها اختصاص نمی دهد،	

شماره الزام	نام الزام
۱۲	**استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱**
۱۵	**قابلیت‌های ضد اکسپلویت ۳**
برنامه کاربردی با امکانات امنیتی که توسط تولیدکننده پلتفرم ارائه شده است، سازگار است.	
۱۶	**قابلیت‌های ضد اکسپلویت ۴**
برنامه کاربردی فایل‌هایی را که توسط کاربر قابل تغییر هستند در دایرکتوری‌هایی می نویسد که حاوی فایل‌های اجرایی‌نبستند، مگر اینکه کاربر به‌طور مستقیم چنین دایرکتوری‌ها را انتخاب نماید.	
۱۷	**قابلیت‌های ضد اکسپلویت ۵**
برنامه کاربردی باقابلیت محافظت از سرریز بافر مبتنی بر پشته کامپایل می شود.	
۱۸	**به‌روزرسانی امن ۱**
برنامه کاربردی باید **این قابلیت را ارائه کند، این قابلیت را برای پلتفرم فراهم نماید** که بروزسانی و وصله های برنامه کاربردی را بررسی نماید. برنامه کاربردی از طریق برنامه ای شبیه Click Once بروزرسانی خود را انجام می دهد.	
۱۹	**به‌روزرسانی امن ۲**
برنامه کاربردی با استفاده از قالب مدیریت بسته که توسط آن پلتفرم پشتیبانی می‌شود، توزیع و منتشر می شود.	
۲۰	**به‌روزرسانی امن ۳**
برنامه کاربردی طوری بسته‌بندی می شود که حذف آن، منجر به پاک شدن تمامی آثار برنامه کاربردی می شود؛ به‌استثناء تنظیمات پیکربندی، فایل‌های خروجی و ثبت وقایع/ ممیزی.	
۲۱	**به‌روزرسانی امن ۴**
برنامه کاربردی کد باینری خود را دانلود، اصلاح، جایگزین یا به‌روزرسانی نمی کند.	
۲۲	**به‌روزرسانی امن ۵**
برنامه کاربردی حداقل یا این قابلیت را ارائه می کند، یا این قابلیت را برای پلتفرم فراهم می نماید تا نسخه فعلی برنامه کاربردی را بازیابی می کند.	

شماره الزام	نام الزام
۱۲	**استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱**
۲۳	**به‌روزرسانی امن ۶**
بسته نصب برنامه کاربردی و نسخه‌های به‌روزرسانی آن به طوردیجیتالی امضا می شوند به طوری که پلتفرم بتواند رمزنگاری آنان را قبل از نصب برنامه کاربردی، چک کند. اکثر DLL ها امضاء شده اند به جز یکی دو مورد خاص.	
۲۴	**استفاده از کتابخانه‌های شخص ثالث ۱**
هدف از این الزام آناست که ارزیاب کتابخانه‌های شخص ثالث غیرضروری یا پیش‌بینی نشده در برنامه کاربردی را تشخیص و ثبت نماید. این شامل کتابخانه‌هایی که جهت امور تبلیغاتی ایجاد شده‌اند نیز می‌شود که می‌تواند تهدیدی برای حریم خصوصی به شمار رود. همچنین شامل تضمین مستندسازی این کتابخانه‌ها برای مواقعی که آسیب‌پذیری‌هایی در آینده کشف شوند نیز است. لیست کتابخانه های شخص ثالث سامانه جامع IGS به شرح زیر می باشد: AcroPDF.dll ActiveQueryBuilder.Core.dll ActiveQueryBuilder.MSSQLMetadataProvider.dll ActiveQueryBuilder.View.dll ActiveQueryBuilder.View.WinForms.dll ActiveReports.Design2.dll ActiveReports.XlsExport.dll Aga.Controls.dll AnexTools.Windows.Component.AnexTree.dll AxInterop.AcroPDFLib.dll AxInterop.SHDocVw.dll CrystalDecisions.CrystalReports.Engine.dll CrystalDecisions.Data.AdoDotNetInterop.dll CrystalDecisions.ReportAppServer.ClientDoc.dll CrystalDecisions.ReportAppServer.CommLayer.dll CrystalDecisions.ReportAppServer.DataDefModel.dll CrystalDecisions.ReportSource.dll CrystalDecisions.Shared.dll CrystalDecisions.VSDesigner.dll CrystalDecisions.Web.dll CrystalDecisions.Windows.Forms.dll DocumentFormat.OpenXml.dll GemBox.ExcelLite.dll ICSharpCode.SharpZipLib.dll	

شماره الزام	نام الزام
۱۲	**استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱**

Interop.AcroPDFLib.dll
Interop.Excel.dll
Interop.Office.dll
Interop.SHDocVw.dll
Interop.VBIDE.dll
Interop.WIA.dll
Interop.Word.dll
itextsharp.dll
itextsharp.pdfa.dll
Janus.Data.v4.dll
Janus.Windows.ButtonBar.v4.dll
Janus.Windows.CalendarCombo.v4.dll
Janus.Windows.Common.v4.dll
Janus.Windows.ExplorerBar.v4.dll
Janus.Windows.FilterEditor.v4.dll
Janus.Windows.GridEX.v4.dll
Janus.Windows.Ribbon.v4.dll
Janus.Windows.Schedule.v4.dll
Janus.Windows.TimeLine.v4.dll
Janus.Windows.UI.v4.dll
log4net.dll
Microsoft.Office.Interop.Word.dll
Microsoft.ReportViewer.Common.dll
Microsoft.ReportViewer.DataVisualization.dll
Microsoft.ReportViewer.ProcessingObjectModel.dll
Microsoft.ReportViewer.WinForms.dll
Newtonsoft.Json.dll
SQLite.Interop.dll
System.Data.SQLite.dll
Word.dll
BouncyCastle.Crypto.dll
DocumentFormat.OpenXml.dll
ICSharpCode.SharpZipLib.dll
Interop.Office.dll
Interop.Word.dll
Microsoft.AnalysisServices.DLL
Newtonsoft.Json.dll
OpenPop.dll
Oracle.ManagedDataAccess.dll
RestSharp.dll

شماره الزام	نام الزام
۱۲	**استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱**
SQLite.Interop.dll System.Data.SQLite.dll WindowsBase.dll	

۶,۴ کلاس کانال‌ها و مسیرهای مورد اعتماد

شماره الزام	نام الزام
۲۵	**حفاظت از تبادل داده‌ها ۱**
برنامه کاربردی بین خود و دیگر محصولات مورد اعتماد IT هیچ داده‌ی حساسی را تبادل نمی‌کند.	