به نام خدا

پروفایل حفاظتی

سامانه مدیریت امنیت سازمانی

آبان ۹۵

نسخه ۱,۱

فهرست

۱ مقدمه

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی را که در این سند برای برآورده کردن الزامات ارائه شده‌اند در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد.

الزامات این سند تکمیل‌کننده سند «پروفایل حفاظتی برنامه‌های کاربردی» برای سامانه مدیریت امنیتی می‌باشد، لذا این نوع سامانه‌ها می‌بایست علاوه بر الزامات این سند، الزامات سند «پروفایل حفاظتی برنامه‌های کاربردی» را نیز برآورده سازند. در این سند الرامات امنیتی سامانه مدیریت امنیت بیان می-شود. مرکز افتا با مشارکت سازمان فناوری اطلاعات این سند را بر اساس سند طرح ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 در راستای این هدف تهیه نموده است. این پروفایل حفاظتی، به بیان الزامات «سامانه مدیریت امنیت» می‌پردازد.

۲ اصطلاحات

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

متدلوژی ارزیابی معیار مشترک[۱] (CEM): متدلوژی ارزیابی معیار مشترک برای ارزیابی امنیت فناوری‌های اطلاعات.

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

پروفایل حفاظتی (PP[۲]): مجموعه‌ای از الزامات امنیتی برای دسته‌ای از محصولات؛ مجموعه‌ای که مستقل از پیاده‌سازی است.

هدف امنیتی (ST[۳]): 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[۴]): مجموعه‌ای از الزامات تضمین که از قسمت سوم از سندهای سه‌گانه «استاندارد ارزیابی معیار مشترک» برگرفته‌شده 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» است.

خلاصه مشخصه محصول[۵] **(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 تاثیر قرار نمی‌دهند. این داده‌ها اطلاعاتی ذخیره‌شده در منابع محصول هستند که توسط کاربران مطابق با الزامات کارکرد امنیتی به‌کاربرده می‌شود. محتویات یک پیام الکترونیک نوعی داده کاربری می‌باشد.

---

[۱] Common Evaluation Methodology(CEM)
[۲] Protection Profile
[۳] Security Target
[۴] Evaluation Assurance Level
[۵] TOE Summary Specification (TSS)

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

موجودیت فعال (Subject): موجودیت فعال، موجودیتی در 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.

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 حمله‌کننده که در این دو مثال رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.

مشخصه‌های امنیتی: می‌تواند شامل مشخصه‌های امنیتی موجودیت فعال (از قبیل شناسه کاربر، کلمه عبور، نقش‌های کاربر، جزئیات واسط کاربر، پیشینه احراز هویت) و یا مشخصه‌های امنیتی غیرفعال (از قبیل نوع، نام و اندازه مستند) باشد.

داده‌های محصول: می‌تواند شامل داده‌های ممیزی، کلیدها، مقادیر تنظیمات محصول و داده‌های احراز هویت و از این نوع داده‌ها باشد.

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

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

۳ شرح محصول

امروزه با رشد روز افزون فناوری اطلاعات و ارتباطات در سازمان‌ها، یکی از مسائل مهمی که در سازمان‌ها باید در نظر گرفته شود امنیت است. از طرفی، خطرات مختلفی از قبیل خطرات داخل و بیرونی، سازمان‌ها را تهدید می‌کنند؛ بنابراین استفاده از تجهیزات و سیاست‌ها و امکانات امنیتی می‌تواند نقش مهمی را در تامین امنیت سازمان‌ها ایفا نماید. یکی از ابزارهای مهم در جلوگیری و کاهش تهدیدات سامانه مدیریت امنیت می‌باشد.

سامانه مدیریت امنیت به سیستم‌هایی اشاره دارد که به منظور مدیریت متمرکز مجموعه‌ای از «دارایی‌های فناوری اطلاعات» در یک سازمان مورد استفاده قرار می‌گیرد. این نوع سامانه‌ها از خط‌مشی‌هایی مانند زیر تعریف می‌شوند:

- **خط‌مشی کنترل دسترسی:** خط‌مشی‌هایی که اجرای عملیات، از سوی یک موجودیت فعال بر روی یک موجودیت غیرفعال را رد یا تایید می‌کند.
- **خط‌مشی شناسایی و اعتبارسنجی:** خط‌مشی‌هایی که پارامترهای لازم برای شناسایی، احراز هویت، اعتبارسنجی و پاسخگویی یک موجودیت فعال را تعریف و نگهداری می‌کنند.
- **خط‌مشی‌های ویژگی‌های موجودیت‌های غیرفعال:** خط‌مشی‌هایی که ویژگی‌های موجودیت‌های غیرفعال را تعریف و نگهداری می‌کنند.
- **خط‌مشی‌های احراز هویت**: خط‌مشی‌هایی که چگونگی احراز هویت کاربران سیستم را تعریف می‌کنند.
- **خط‌مشی‌های پیکربندی امن**: خط‌مشی‌هایی که اصول اولیه پیکربندی برای دارایی‌های IT را تعریف می‌کنند.
- **خط‌مشی‌های ممیزی**: خط‌مشی‌هایی که چگونگی جمع‌آوری، یکپارچه‌سازی، گزارش‌دهی و نگهداری داده‌های ممیزی را تعریف می‌کنند.

سامانه مدیریت امنیت که خط‌مشی‌های مختلف را مدیریت و اعمال می‌کند، امنیت را به گونه‌های زیر پیاده‌سازی می‌کند:

- **پیشگیرانه**[۱]: در این روش با نقض یک خط‌مشی، اجرای عملیات به روی دارایی‌های IT ممنوع خواهد شد.

[۱] -Preventive

- **شناساگرانه[۱]:** در این روش رفتار کاربران و دارایی‌های IT، ممیزی و جمع‌آوری می‌گردد، بنابراین الگوی یک رفتارناامن، بدخواهانه و یا سایر رفتارهای نامتناسب در سامانه شناسایی خواهد شد.
- **واکنش‌گرانه[۲]:** دارایی‌های IT با یک قوانین امن مرکزی تعریف‌شده در سازمان مقایسه می‌شوند و عملیات در صورتی انجام می‌شود که تفاوت‌ها شناسایی شود.

به‌طور کلی، سامانه‌های مدیریت امنیت دارای سه نوع قابلیت می‌باشند. نوع اول، تعریف خط‌مشی، برای تعریف خط‌مشی‌های متمرکز سازمانی که برای کنترل کردن رفتار یک مجموعه از دارایی‌های IT استفاده می‌شود، کاربرد دارد. این موضوع با مثال‌های زیر نشان داده می‌شود:

- یک محصول مدیریت پیکربندی امن، یک خط‌مشی تعریف می‌کند تا یک مجموعه مورد تایید از دارایی‌های نرم‌افزاری و یا پیکربندی برنامه‌های موجود در یک سیستم را کنترل کند.
- یک محصول مدیریت خط‌مشی می‌تواند عملیاتی را تعریف کند که بر اساس کاربری که درخواست می‌دهد و موجودیت غیرفعالی که درخواست برای آن صادر می‌شود، مجاز یا غیرمجاز شناخته شود.

قابلیت دوم، بکار بردن خط‌مشی می‌باشد که یک خط‌مشی تعریف‌شده را ذخیره کرده و آن را به‌طور مداوم عملیاتی می‌کند. این موضوع با مثال‌های زیر نشان داده‌شده است:

- یک محصول کنترل دسترسی که در یک سامانه قرار می‌گیرد یک خط‌مشی کنترل دسترسی از مدیریت خط‌مشی‌ها دریافت می‌کند، سپس آن را ذخیره نموده و اطمینان حاصل می‌کند که تمام موجودیت‌های فعال این خط‌مشی را رعایت کرده تا زمانی که دستور دیگری صادر شود.

---

۱ -Detective

۲ -Reactive

- یک محصول کنترل دسترسی که جلوگیری از نشت داده را در یک سامانه عملیاتی می‌کند، می‌تواند یک ویژگی تعریف‌شده از یک موجودیت غیرفعال دریافت کند که سطوح مختلفی از حساسیت را به داده‌ها نسبت می‌دهد، آنگاه این خط‌مشی ذخیره می‌شود و به‌طور مداوم بر اساس سطح حساسیت داده‌ها، مانع خروج آن‌ها از سامانه می‌شود.

نوع سوم از قابلیت‌ها، اعمال خط‌مشی‌ها می‌باشد که در نتیجه‌ی اجرای یک پرس‌وجو یا دستوری از منبع آن خط‌مشی‌ها می‌باشد که، در زمان مناسب اعمال می‌شود. این مسئله در مثال‌های زیر نشان داده‌شده است:

- یک مدیر سیستم تلاش می‌کند تا برای مدیریت یک محصول مدیریت امنیت، وارد سیستم شود. درخواست احراز هویت او در یک سرور احراز هویت ثبت می‌شود تا با توجه به خط‌مشی احراز هویت تعریف‌شده، درخواست مدیر را رد یا تایید کند. محصول مدیریت خط‌مشی آنگاه تصمیم سرور احراز هویت را اعمال می‌کند و بر اساس آن اجازه دسترسی را صادر می‌کند.
- یک محصول مدیریت پیکربندی امن، یک خط‌مشی تعریف می‌کند که از بروز بودن نرم افزار بکار گرفته‌شده اطمینان حاصل کند. پس از بررسی مشخص می‌شود که محصول کنترل دسترسی از یک نسخه قدیمی است. محصول مدیریت پیکربندی امن به محصول کنترل دسترسی دستوری صادر می‌کند تا از یک بسته تکمیلی استفاده کند. خط‌مشی پیکربندی امن متعاقبا از طریق محصول کنترل دسترسی اعمال می‌شود.

۱,۳ مروری بر پروفایل حفاظتی کنترل دسترسی سامانه مدیریت امنیت

این پروفایل بر روی تصمیمات کنترل دسترسی و اعمال آن‌ها تمرکز دارد. محصولی که مطابق این پروفایل حفاظتی باشد، یک خط‌مشی کنترل دسترسی را تعریف و اعمال می‌کند که با این کار، امنیت پیشگیرانه‌ای را در سازمان بکار می‌گیرد. محصولی که مطابق با این پروفایل حفاظتی باشد، می‌بایست درخواست‌هایی که برای دسترسی به انواع منابع تعریف‌شده (مانند فایل‌های سیستمی برروی یک ایستگاه کاری و یا یک وب‌سایت بر روی یک اینترانت سازمانی) می‌شود را بررسی و تایید یا رد شدن درخواست را تعیین کند. در یک سامانه مدیریت امنیت، این قابلیت، نقطه تصمیم خط‌مشی (PDP[1]) نامیده

[1]-Policy decision point

می‌شود. آنگاه نتیجه‌ی تصمیم اعمال می‌شود و یا اینکه به یک موجودیت مورد اعتماد دیگر برای اعمال خط‌مشی، فرستاده می‌شود. در یک سامانه مدیریت امنیت، این قابلیت، نقطه اعمال خط‌مشی (PEP[1]) نامیده می‌شود. محصولاتی که با این پروفایل سازگار هستند، دارای هردو قابلیت تصمیم خط‌مشی و اعمال خط‌مشی می‌باشند. برخی از محصولات، تنها دارای تصمیم خط‌مشی هستند و اعمال خط‌مشی را به محیط عملیاتی واگذار می‌کنند. در این گونه موارد تنها راه ارزیابی محصول از طریق این پروفایل این است که محدوده مؤلفه‌ی عملیاتی اعمال خط‌مشی، به‌عنوان محصول تعیین شود.

توجه به تفاوت کنترل دسترسی و کنترل دسترسی سامانه مدیریت امنیت، مسئله‌ی مهمی می‌باشد:

کنترل دسترسی سامانه مدیریت امنیت به صورت متمرکز تعریف‌شده است: کنترل دسترسی سامانه مدیریت امنیت یک خط‌مشی متمرکز را اعمال می‌کند، در صورتی که یک سیستم عامل یک خط‌مشی محلی را اعمال می‌کند (به‌طور مثال خط‌مشی‌هایی که به‌صورت محلی و منحصراً برای همان سیستم‌عامل تعریف‌شده‌اند).

مؤلفه‌های کنترل دسترسی به عنوان بخشی از مؤلفه‌های سامانه مدیریت امنیت به حساب می‌آیند. یک مؤلفه کنترل دسترسی توسط سامانه مدیریت امنیت باید قابلیت‌های زیر را داشته باشد:

- تعریف خط‌مشی متمرکز: یک قابلیت مدیریت خط‌مشی متمایز این است که مجموعه قوانینی را برای تصمیمات خط‌مشی محصول کنترل دسترسی تعریف نماید. این قوانین شامل عملیات-موجودیت‌های فعال و موجودیت‌های غیرفعال خواهد بود. موجودیت‌های فعال و غیرفعال توسط مشخص‌های تعیین‌شده سازمانی (از قبیل نام کاربری، موقعیت جغرافیایی، آدرس URL از یک منبع محافظت‌شده و زمان) تعریف‌شده هستند.
- تعریف موجودیت فعال مرکزی: یک قابلیت مدیریت شناسایی و احراز هویت باید یک تعریف واحد از کاربران داشته باشد.
- تعریف موجودیت غیرفعال: در بیشتر موارد انتظار می‌رود که مشخصه‌های موجودیت غیرفعال که توسط محصول کنترل دسترسی بررسی می‌شوند بخش ذاتی موجودیت غیرفعال در محیط عملیاتی خواهد بود. به عنوان مثال، مدیر بررسی وب ممکن است URL صفحه وب یا زمان دسترسی به آن را بررسی نماید.

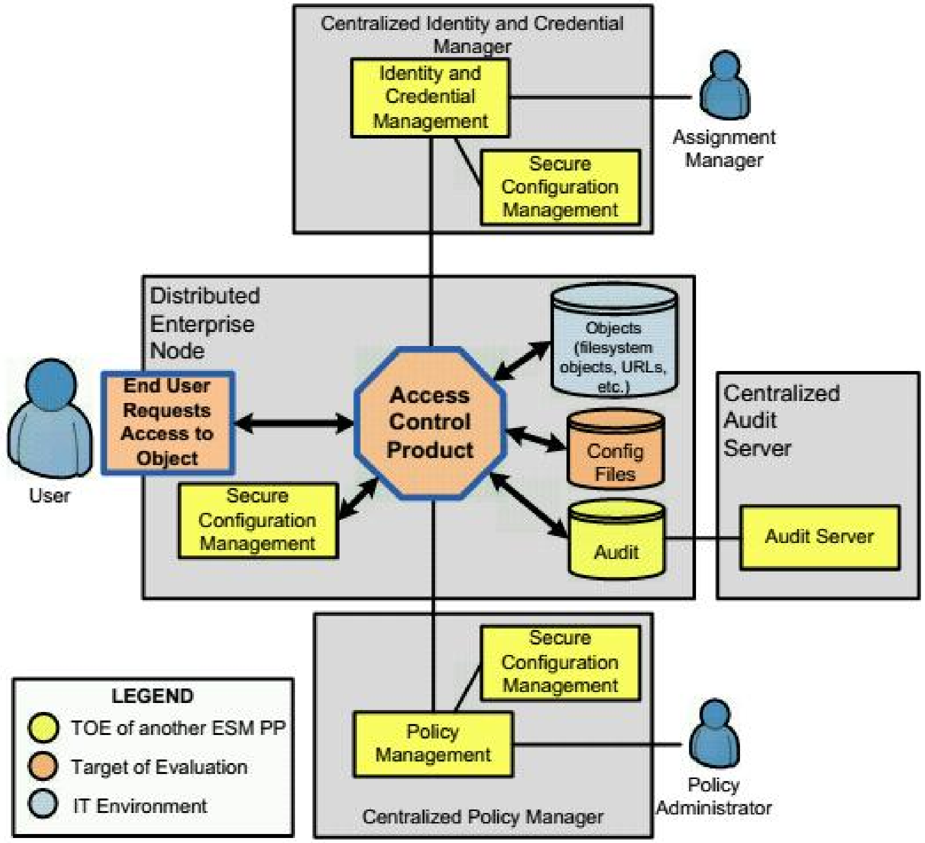
[1]-Policy Enforcement point

- اطمینان از شناسایی موجودیت فعال به‌طور متمرکز: یک سرور احراز هویت متمایز و جدا برای احراز هویت موجودیت‌های فعال مورد استفاده قرار می‌گیرد که در مورد معتبر بودن هویت آن‌ها تصمیم‌گیری می‌کند.
- پشتیبانی از ممیزی متمرکز: یک سرور ممیزی جدا و متمایز داده‌های ممیزی را برای اهداف گزارش‌گیری و مدیریت حوادث جمع‌آوری می‌نماید.
- پشتیبانی از مدیریت پیکربندی امن: یک محصول مدیریت پیکربندی امن جدا باید پیکربندی محصول کنترل دسترسی را بررسی نموده تا اطمینان حاصل شود که با خط‌مشی امنیتی سازمان منطبق می‌باشد.

شکل ۱ شمایی از سامانه مدیریت امنیت است که نشان می‌دهد که چگونه مؤلفه‌های این سامانه به یکدیگر مرتبط هستند.

هنگام تهیه سند هدف امنیتی مطابق با این پروفایل حفاظتی، نویسنده باید به‌طور واضح انواع تکنولوژی که در محصول بکار رفته است را شناسایی نماید. تکنولوژی‌ها باید الزامات حفاظت از داده‌های کاربری را تحت پوشش قرار دهند.

بدون در نظر گرفتن نوع تکنولوژی، ضروری است که محصول موجودیت‌های فعال و مشخصه‌های تعریف‌شده در سازمان‌ها را مطابق با این پروفایل حفاظتی مدیریت نماید. نویسنده هدف امنیتی باید داده‌های سازمانی را که در محصول استفاده خواهد شد را تعریف نماید. منابع امنی که داده‌ها را دریافت کرده و سازوکار تفسیر داده‌ها (از قبیل SAML یا گواهینامهX.509) باید ذکر شود.



شکل ۱- شمایی از سامانه مدیریت امنیت

کنترل دسترسی مبتنی بر میزبان:

محصولات کنترل دسترسی مبتنی بر میزبان برای اعمال کنترل دسترسی انتزاعات سازمانی طراحی‌شده‌اند. قابلیت‌هایی که این نوع محصول باید دارا باشند به شرح زیر است:

- خواندن، نوشتن، ویرایش، حذف و اجرای عملیات در برابر فایل‌ها
- خواندن، نوشتن، ویرایش، حذف و اجرای عملیات در برابر پروسه‌های قابل اجرا
- درج کردن و ویرایش عملیات در برابر پارامترهای پیکربندی سیستم
- خاموش کردن و راه‌اندازی مجدد عملیات در برابر سیستمی که محصول بر روی آن قرار دارد

کنترل دسترسی مبتنی بر میزبان ممکن است برای محدودسازی مجوزهای مدیریتی سیستم در محیط عملیاتی مورد استفاده قرار بگیرد (مانند حساب کاربری root سیستم عامل).

کنترل دسترسی مبتنی بر وب:

محصول کنترل دسترسی مبتنی بر وب یک برنامه کاربردی است که درخواست‌های موجودیت فعال را برای تعامل با محتویات مبتنی بر وب بررسی کرده و بر اساس اعمال یک خط‌مشی مشخص می‌کند که آیا درخواست را رد و یا اجازه دهد. معمولا بر روی یک سرور مرکزی قرار دارد که درخواست‌های موجودیت فعال را مسیردهی می‌کند. حداقل‌ترین قابلیتی که محصول سامانه مدیریت امنیت کنترل دسترسی مبتنی بر وب باید دارا باشد به شرح زیر است:

- عملیات POST، HTTP GET، HEAD در برابر موجودیت‌های غیرفعال وب
- اجرای عملیات در برابر اسکریپت‌هایی که در موجودیت‌های غیرفعال وبی گنجانده شده‌اند.

همچنین یک محصول کنترل دسترسی مبتنی بر وب، ممکن است به‌طور اختیاری خط‌مشی را اعمال نماید که بر اساس روز و زمان عملیاتی آغاز شود.

جلوگیری از نشت داده‌ها:

هدف اصلی از سیستم جلوگیری از نشت داده‌ها برای شناسایی و وجود دسترسی و اعمال آن برای اطلاعات حساس سازمانی و کاهش ریسک افشای غیرمجاز اطلاعات است. در حال حاضر محصول DLP به دو صورت تحت شبکه و نقطه انتهائی[۱] وجود دارد.

محصولات DLP مبتنی بر شبکه در موقعیت‌های شبکه قرار دارند و تقریبا همانند دیواره آتش رفتار می‌کنند.

راه‌حل‌های DLP مبتنی بر نقطه انتهائی، محصولاتی هستند که بر روی میزبان نصب‌شده و به طور محلی بر روی سیستم‌عامل اجراشده تا اطلاعات حساس ذخیره‌شده را شناسایی، ممیزی نمایند و بر روی کامپیوتر کاربر یا سرور شبکه اجرا می‌شود. معمولا DLP مبتنی بر نقطه انتهائی، کنترل دسترسی اطلاعات را از طریق قابلیت‌های کپی/چسباندن، چاپ کردن، عملیات فایل (ذخیره، ویرایش، حذف و باز کردن)، نوشتن بر روی CD/DVD و کنترل دستگاه USB انجام می‌دهند.

یک محصول DLP حداقل قابلیت‌های زیر را باید دارا باشد:

- کنترل دسترسی عملیات نوشتن در برابر بافر یک پرینتر
- کنترل دسترسی عملیات خواندن و نوشتن در برابر دستگاه‌های قابل حمل
- کنترل دسترسی عملیات کپی و چسباندن درون برنامه و یا بین برنامه‌ها
- کنترل دسترسی ارسال عملیات در برابر سرویس ایمیل
- کنترل دسترسی عملیات HTTP POST در برابر محتویات وب

از طرفی خط‌مشی مورد استفاده در محصول DLP باید قابلیت تعریف، شناسایی باشد و همچنین قادر به حفاظت از فهرستی از انواع داده‌ها در برابر از دست رفتن داده‌ها باشد.

[۱] Endpoint

در نهایت محصول DLP باید قادر به بازرسی فایل‌های داده‌ها از قبیل پایگاه داده‌ها، PDF ها و اسناد Word باشد تا در صورت وجود اطلاعات حساس، محافظت نماید؛ بنابراین محصول DLP داده‌های موجودیت‌های غیرفعال را باید براساس الگو، امضاء یا از طریق درهم‌سازی در محتویاتی که به‌طور مستقیم قابل بازرسی نیستند، شناسایی نماید؛ بنابراین باید موجودیت‌های غیرفعال رمزشده را تشخیص و بر اساس خط مش اجازه و یا مانع انتقال آن‌ها گردند.

۴ تعریف مسائل امنیتی

۱,۴ فرضیات

A.TYPE	توضیحات
A.CONNECTIONS	فرض می‌شود که هدف ارزیابی به گونه‌ای به شبکه‌های جداگانه متصل می‌گردد که از قابل اجرا بودن خطمشی‌های امنیتی هدف ارزیابی بر روی تمام جریان ترافیک شبکه در بین شبکه‌های متصل اطمینان حاصل نماید.
A.CRYPTO	هدف ارزیابی از رمزنگاری اولیه ارائه‌شده توسط محیط عملیاتی جهت خدمات رمزنگاری استفاده خواهد نمود.
A.POLICY	هدف ارزیابی اطلاعات مربوط به خط‌مشی را از محیط عملیاتی دریافت می‌نماید.
A.USERID	هدف ارزیابی اطلاعات شناسایی معتبر را از محیط عملیاتی دریافت خواهد نمود.
A.INSTALL	یک مدیر شایسته و مورد اعتماد وجود خواهد داشت که از راهنمایی‌های ارائه‌شده به منظور نصب هدف ارزیابی پیروی خواهد کرد.

۲,۴ تهدیدات

T.TYPE	توضیحات
T.UNAUTH	کاربر متخاصم ممکن است به موجودیت غیرفعال در محیط عملیاتی دسترسی پیدا نموده و سبب افشاء داده حساس شوند یا بر روی عملکرد سامانه اثر منفی بگذارد.

T.DISABLE	کاربر متخاصم ممکن است عملکرد هدف ارزیابی را متوقف نموده یا خاتمه دهد، بنابراین قادر به اعمال کنترل دسترسی‌اَش بر روی محیط یا داده حفاظت‌شده توسط هدف ارزیابی نخواهد بود.
T.NOROUTE	کاربر متخاصم ممکن است سبب قطع اتصال هدف ارزیابی به منبع اجراکننده خط‌مشی‌ها شود و بر عملکرد کنترل دسترسی تاثیر منفی بگذارد.
T.EAVES	کاربر مخرب می‌تواند ترافیک شبکه را شنود نماید تا به داده هدف ارزیابی دسترسی غیر مجازی پیدا نماید.
T.FALSIFY	کاربر مخرب می‌تواند هویت هدف ارزیابی را تحریف نماید و به سامانه مدیریت خط‌مشی نسبت به اعمال خط‌مشی توسط هدف ارزیابی اطمینان کاذب دهد.
T.FORGE	کاربر مخرب ممکن است خط‌مشی نادرستی ایجاد نموده و آن را برای اجرا به هدف ارزیابی ارسال نماید و سبب تغییرات منفی در عملکرد آن گردد.
T.MASK	کاربر مخرب ممکن است تلاش نماید تا اقداماتش را بپوشاند تا موجب ثبت نادرست داده ممیزی یا به طور کل ثبت نشدن آن گردد.
T.OFLOWS	کاربر مخرب ممکن است تلاش نماید تا با ارائه داده خط‌مشی ناصحیح به هدف ارزیابی، رفتار خط‌مشی کنترل دسترسی آن را تغییر دهد.

۳٫۴ خط‌مشی‌های امنیتی

P.TYPE	توضیحات
P.ACCESS_BANNER	هدف ارزیابی باید پرچم‌های اولیه را نمایش دهد که توصیف‌کننده محدودیت‌های استفاده، توافقات قانونی یا هرگونه اطلاعات مناسب دیگری است که کاربران با دستیابی به هدف ارزیابی با آن‌ها موافقت می‌نمایند.
P.UPDATEPOL	سازمان تمام تلاش خود را می‌نماید تا اطمینان حاصل شود که هدف ارزیابی با داده‌های خط‌مشی مربوطه به‌روز شده است.

۵ اهداف امنیتی

۱٫۵ اهداف امنیتی هدف ارزیابی

O.TYPE	توضیحات
O.CRYPTO (optional)	هدف ارزیابی از الگوریتم‌های رمزنگاری استفاده خواهد نمود که ارائه‌دهنده سرویس‌هایی همچون اطمینان از محرمانگی و صحت ارتباطات می‌باشد.
O.DATAPROT	هدف ارزیابی با اعمال نمودن خط‌مشی کنترل دسترسی تولیدشده توسط محصول مدیریت خط‌مشی، از تغییرات غیرمجاز داده‌ها محافظت خواهد نمود.
O.INTEGRITY	هدف ارزیابی قادر خواهد بود تا صحت داده‌های منتقل‌شده از مؤلفه‌های محیط عملیاتی را بررسی نماید.
O.MAINTAIN	در صورتی که هدف ارزیابی قادر به برقراری ارتباط با محصول مدیریت خط‌مشی (ارائه‌دهنده خط‌مشی) نباشد، می‌تواند خط‌مشی کنترل دسترسی را حفظ نماید.
O.MNGRID	هدف ارزیابی پیش از پذیرش داده خط‌مشی از محصول مدیریت خط‌مشی، قادر به شناسایی و مجاز نمودن محصول می-باشد.
O.MONITOR	هدف ارزیابی عملکرد خودش را برای فعالیت‌های غیرمعمول مانیتور می‌نماید (به طور مثال، ارائه معیاری برای تولید و ثبت رویدادهای مربوطه امنیتی می‌باشد؛ که تلاش‌های کاربران جهت دسترسی به منابع محافظت‌شده هدف ارزیابی را شناسایی می‌نماید.)
O.OFLOWS	هدف ارزیابی قادر به تشخیص و رد نمودن ورودی‌های نامعتبر و مخرب ارائه‌شده توسط کاربران می‌باشد.
O.PROTCOMMS	هدف ارزیابی برای سرپرست، دیگر بخش‌های هدف ارزیابی توزیع‌شده و موجودیت IT مجاز کانال ارتباطی محافظت‌شده ارائه خواهد نمود.
O.RESILIENT (optional)	در صورتی که هدف ارزیابی، واسط اقدام انجام‌گرفته توسط کاربر در قبال منابع سیستم عامل باشد، سرپرست سیستم یا کاربر نباید مجاز به انجام عملیاتی در محیط عملیاتی باشند که عملکرد هدف ارزیابی را تغییر داده یا غیرفعال نماید.
O.SELFID	هدف ارزیابی در هنگام ارسال وصول از دریافت خط‌مشی جدید، قادر به تائید هویتش به محصول مدیریت خط‌مشی

	خواهد بود.

۲,۵ اهداف امنیتی محیط عملیاتی

OE.TYPE	توضیحات
OE.CONNECTIONS	سرپرستان هدف ارزیابی اطمینان خواهند داد که هدف ارزیابی به صورتی نصب می‌گردد که اجازه خواهد داد خط مشی-های هدف ارزیابی بر روی جریان ترافیک شبکه در میان شبکه‌های متصل شده، اجرا گردد.
OE.CRYPTO (optional)	محیط عملیاتی رمزنگاری اولیه‌ای ارائه خواهد نمود که برای ارائه خدماتی مانند تضمین محرمانگی و یکپارچگی اطلاعات استفاده می‌شود.
OE.INSTALL	مسئولان هدف ارزیابی باید نسبت به دریافت، نصب، مدیریت و کارکرد هدف ارزیابی به صورت امن اطمینان دهند.
OE.POLICY	محیط عملیاتی اجراکننده‌ی سیاست اجراشده توسط هدف ارزیابی می‌باشد.
OE.PROTECT (optional)	محیط عملیاتی هدف ارزیابی از تغییرات غیر مجاز و دسترسی به توابع و داده‌های خود را محافظت خواهد کرد.
OE.SYSTIME	محیط عملیاتی فراهم‌کننده‌ی اطلاعات زمانی قابل اطمینان برای هدف ارزیابی خواهد بود.
OE.USERID	محیط عملیاتی باید قادر به شناسایی درخواست دسترسی کاربر به منابعی باشد که توسط کارکرد امنیتی محصول محافظت‌شده است

۶ الزامات کارکرد امنیتی

این بخش معرف الزامات کارکرد امنیتی برای هدف ارزیابی می‌باشد. الزامات توابع امنیتی هدف ارزیابی که در جدول زیر عنوان شده‌اند، در زیربخش‌هایی که در ادامه آمده است، توصیف می‌گردند.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**تولید داده ممیزی ۱**	FAU_GEN.1.1
۲	**تولید داده ممیزی ۲**	FAU_GEN.1.2
۳	**ممیزی انتخابی ۱**	FAU_SEL.1.1
۴	**ذخیره‌سازی رویدادهای ممیزی ۱**	FAU_STG.1.1
۵	**ذخیره‌سازی رویدادهای ممیزی ۲**	FAU_STG.1.2
۶	**ذخیره‌سازی رویدادهای ممیزی خارجی ۱**	FAU_STG_EXT.1.1
۷	**ذخیره‌سازی رویدادهای ممیزی خارجی ۲**	FAU_STG_EXT.1.2
۸	**ذخیره‌سازی رویدادهای ممیزی خارجی ۳**	FAU_STG_EXT.1.3
۹	**عدم انکار اطلاعات توسط گیرنده ۴**	FCO_NRR.2.1
۱۰	**عدم انکار اطلاعات توسط گیرنده ۵**	FCO_NRR.2.2
۱۱	**عدم انکار اطلاعات توسط گیرنده ۶**	FCO_NRR.2.3
۱۲	**خط‌مشی کنترل دسترسی ۱**	FDP_ACC.1.1
۱۳	**عملیات کنترل دسترسی ۱**	FDP_ACF.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۴	**مدیریت احراز هویت ناموفق ۱**	FIA_AFL.1.1
۱۵	**مدیریت احراز هویت ناموفق ۲**	FIA_AFL.1.2
۱۶	**احراز هویت کاربر ۱**	FIA_UAU.1.1
۱۷	**احراز هویت کاربر ۲**	FIA_UAU.1.2
۱۸	**احراز هویت کاربر ۱۰**	FIA_UAU.1.7
۱۹	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱**	FIA_USB.1.1
۲۰	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر۲**	FIA_USB.1.2
۲۱	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳**	FIA_USB.1.3
۲۲	**مدیریت کارکرد در محصول ۱ (۱)**	FMT_MOF.1.1 (1)
۲۳	**مدیریت کارکرد در محصول ۱ (۲)**	FMT_MOF.1.1(2)
۲۴	**مدیریت مشخصه‌های امنیتی ۱**	FMT_MSA.1.1
۲۵	**مدیریت مشخصه‌های امنیتی ۳**	FMT_MSA.3.1
۲۶	**مدیریت مشخصه‌های امنیتی ۴**	FMT_MSA.3.2
۲۷	**کارکرد مدیریتی محصول ۱**	FMT_SMF.1.1
۲۸	**نقش‌های امنیتی ۱**	FMT_SMR.1.1
۲۹	**نقش‌های امنیتی ۲**	FMT_SMR.1.2
۳۰	**مدیریت داده‌های محصول ۱**	FMT_MTD.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۳۱	**مهرهای زمانی ۱**	FPT_STM.1.1
۳۲	**حفاظت از کلمه عبور سرپرست ۱**	FPT_APW_EXT.1.1
۳۳	**حفاظت از کلمه عبور سرپرست ۲**	FPT_APW_EXT.1.2
۳۴	**حفظ وضعیت امن در زمان شکست ۲**	FPT_FLS_EXT.1.1
۳۵	**تشخیص تکرار ۱**	FPT_RPL.1.1
۳۶	**تشخیص تکرار ۲**	FPT_RPL.1.2
۳۷	**محافظت از داده‌های محصول (کلیدهای متقارن) ۱**	FPT_SKP_EXT.1.1
۳۸	**تحمل خطا ۱**	FRU_FLT.1.1
۳۹	**کانال مطمئن ۱**	FTP_ITC.1.1
۴۰	**کانال مطمئن ۲**	FTP_ITC.1.2
۴۱	**کانال مطمئن ۳**	FTP_ITC.1.3
۴۲	**مسیر مطمئن ۱**	FTP_TRP.1.1
۴۳	**مسیر مطمئن ۲**	FTP_TRP.1.2
۴۴	**مسیر مطمئن ۳**	FTP_TRP.1.3
۴۵	**شناسایی موجودیت غیرفعال ۱**	ESM_DSC.1.1
۴۶	**شناسایی موجودیت غیرفعال ۲**	ESM_DSC.1.2
۴۷	**شناسایی موجودیت فعال ۱**	ESM_EID.2.۱
۴۸	**شناسایی موجودیت فعال ۲**	ESM_EID.2.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۴۹	**تعریف مشخصات موجودیت غیرفعال ۱**	ESM_ATD.1.1
۵۰	**تعریف مشخصات موجودیت غیرفعال ۲**	ESM_ATD.1.۲
۵۱	**شناسایی کاربر و موجودیت امن ۱**	ESM_EAU.2.1
۵۲	**شناسایی کاربر و موجودیت امن ۲**	ESM_EAU.2.2
۵۳	**تعریف مشخصات کاربر در محیط عملیاتی ۱**	ESM_ICD.1.1
۵۴	**تعریف مشخصات کاربر در محیط عملیاتی ۲**	ESM_ICD.1.2
۵۵	**تعریف مشخصات کاربر در محیط عملیاتی ۳**	ESM_ICD.1.3
۵۶	**تعریف مشخصات کاربر در محیط عملیاتی ۴**	ESM_ICD.1.4
۵۷	**تعریف مشخصات کاربر در محیط عملیاتی ۵**	ESM_ICD.1.5
۵۸	**تعریف مشخصات کاربر در محیط عملیاتی ۶**	ESM_ICD.1.6
۵۹	**تعریف مشخصات کاربر در محیط عملیاتی ۷**	ESM_ICD.1.7
۶۰	**تعریف مشخصات کاربر در محیط عملیاتی ۸**	ESM_ICD.1.8
۶۱	**انتقال داده‌های امنیتی کاربر به موجودیت امن ۱**	ESM_ICT.1.1
۶۲	**قفل‌کردن و خاتمه دادن به نشست‌ها ۵**	FTA_SSL.3.1
۶۳	**قفل‌کردن و خاتمه دادن به نشست‌ها ۶**	FTA_SSL.4.1
۶۴	**پیغام‌های هشدار در رابطه با استفاده محصول ۱**	FTA_TAB.1.1
۶۵	**برقراری نشست ۱**	FTA_TSE.1.1
۶۶	**قفل‌کردن و خاتمه دادن به نشست‌ها ۷**	FTA_SSL_EXT.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
	پیوست یک: الزامات رمزنگاری	
۶۷	**مدیریت کلید رمزنگاری ۱**	FCS_CKM.1.1
۶۸	**مدیریت کلید رمزنگاری ۶**	FCS_CKM_EXT.4.1
۶۹	**عملیات رمزنگاری ۱(۱) – رمزنگاری و رمزگشایی**	FCS_COP.1.1(1)
۷۰	**عملیات رمزنگاری ۱(۲)- امضاء دیجیتال**	FCS_COP.1.1(2)
۷۱	**عملیات رمزنگاری ۱(۳) – درهم‌سازی**	FCS_COP.1.1(3)
۷۲	**عملیات رمزنگاری۱(۴)- اصالت‌سنجی پیام**	FCS_COP.1.1(4)
۷۳	**الزامات پروتکل HTTPS (۱)**	FCS_HTTPS_EXT.1.1
۷۴	**الزامات پروتکل HTTPS (۲)**	FCS_HTTPS_EXT.1.2
۷۵	**الزامات پروتکل IPSEC (۱)**	FCS_IPSEC_EXT.1.1
۷۶	**الزامات پروتکل IPSEC (۲)**	FCS_IPSEC_EXT.1.2
۷۷	**الزامات پروتکل IPSEC (۳)**	FCS_IPSEC_EXT.1.3
۷۸	**الزامات پروتکل IPSEC (۴)**	FCS_IPSEC_EXT.1.4
۷۹	**الزامات پروتکل IPSEC (۵)**	FCS_IPSEC_EXT.1.5
۸۰	**الزامات پروتکل IPSEC (۶)**	FCS_IPSEC_EXT.1.6
۸۱	**الزامات پروتکل IPSEC (۷)**	FCS_IPSEC_EXT.1.7
۸۲	**الزامات پروتکل IPSEC (۸)**	FCS_IPSEC_EXT.1.8
۸۳	**تولید بیت تصادفی ۱**	FCS_RBG_EXT.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۸۴	**تولید بیت تصادفی ۲**	FCS_RBG_EXT.1.۲
۸۵	**الزامات پروتکل SSH(۱)**	FCS_SSH_EXT.1.1
۸۶	**الزامات پروتکل SSH(۲)**	FCS_SSH_EXT.1.2
۸۷	**الزامات پروتکل SSH(۳)**	FCS_SSH_EXT.1.3
۸۸	**الزامات پروتکل SSH(۴)**	FCS_SSH_EXT.1.4
۸۹	**الزامات پروتکل SSH(۵)**	FCS_SSH_EXT.1.5
۹۰	**الزامات پروتکل SSH(۶)**	FCS_SSH_EXT.1.6
۹۱	**الزامات پروتکل SSH(۷)**	FCS_SSH_EXT.1.7
۹۲	**الزامات پروتکلTLS/ احراز هویت ۱**	FCS_TLS_EXT.1.8
	پیوست دو	
	الزامات کنترل دسترسی مبتنی بر میزبان	
۹۳	**خط‌مشی کنترل دسترسی ۱**	FDP_ACC.1.1
۹۴	**عملیات کنترل دسترسی ۱**	FDP_ACF.1.1
۹۵	**عملیات کنترل دسترسی ۲**	FDP_ACF.1.2
۹۶	**عملیات کنترل دسترسی ۳**	FDP_ACF.1.3
۹۷	**عملیات کنترل دسترسی ۴**	FDP_ACF.1.4
۹۸	**خط‌مشی کنترل دسترسی ۱ (۲)**	FDP_ACC.1.1(2)
۹۹	**عملیات کنترل دسترسی ۱ (۲)**	FDP_ACF.1.1(2)

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۰۰	**عملیات کنترل دسترسی ۲ (۲)**	FDP_ACF.1.2(2)
۱۰۱	**عملیات کنترل دسترسی ۳ (۲)**	FDP_ACF.1.3(2)
۱۰۲	**عملیات کنترل دسترسی ۴ (۲)**	FDP_ACF.1.4(2)
	الزامات کنترل دسترسی مبتنی بر وب	
۱۰۳	**خط‌مشی کنترل دسترسی ۱**	FDP_ACC.1.1
۱۰۴	**عملیات کنترل دسترسی ۱**	FDP_ACF.1.1
۱۰۵	**عملیات کنترل دسترسی ۲**	FDP_ACF.1.2
۱۰۶	**عملیات کنترل دسترسی ۳**	FDP_ACF.1.3
۱۰۷	**عملیات کنترل دسترسی ۴**	FDP_ACF.1.4
	الزامات کنترل دسترسی جلوگیری از نشت داده‌ها	
۱۰۸	**خط‌مشی کنترل دسترسی ۱**	FDP_ACC.1.1
۱۰۹	**عملیات کنترل دسترسی ۱**	FDP_ACF.1.1
۱۱۰	**عملیات کنترل دسترسی ۲**	FDP_ACF.1.2
۱۱۱	**عملیات کنترل دسترسی ۳**	FDP_ACF.1.3
۱۱۲	**عملیات کنترل دسترسی ۴**	FDP_ACF.1.4
	الزامات خود پایشی	
۱۱۳	**حفظ وضعیت امن در زمان شکست ۱**	FPT_FLS.1.1

۱,۶ کلاس ممیزی امنیت

شماره الزام	نام الزام
۱	**تولید داده ممیزی امنیت (۱)**

محصول باید بتوانند از رویدادهای قابل ممیزی زیر یک رکورد ممیزی تولید نمایند:

- آغاز و اتمام توابع ممیزی؛
- تمامی رویدادهای قابل ممیزی که در جدول زیر آمده است و
- [اختصاص: دیگر رویدادهای قابل ممیزی]

نام الزام	رویداد	توضیحات اضافی
ممیزی انتخابی ۱	تمامی تغییرات در پیکربندی ممیزی	هیچ
ذخیره‌سازی رویدادهای ممیزی خارجی	آغاز و اتمام ارتباطات با سرور ممیزی	شناسایی سرور ممیزی
عدم انکار اطلاعات توسط گیرنده		شناسایی اطلاعات، مقصد و یک کپی از رسید
مدیریت کلید رمزنگاری ۱ (اختیاری)	شکست هنگام تولید کلید	
مدیریت کلید رمزنگاری ۶ (اختیاری)	شکست هنگام تخریب کلید	درخواست موجودیت فعال، دلیل تخریب، شناسایی موجودیت غیرفعال

عملیات رمزنگاری ۱(۱) (اختیاری)	شکست در رمزنگاری یا رمزگشایی	حالت[1] رمزنگاری عملیات، شناسه/ نام موجودیت غیرفعال در حال رمزگذاری/رمزگشایی
عملیات رمزنگاری ۱(۲)(اختیاری)	شکست در امضای دیجیتال	حالت رمزنگاری عملیات، شناسه/ نام موجودیت غیرفعال در حال امضاء/شناسایی شدن
عملیات رمزنگاری ۱(۳) (اختیاری)	شکست در درهم‌سازی	حالت رمزنگاری عملیات، شناسه/ نام موجودیت غیرفعال در حال درهم‌سازی
عملیات رمزنگاری ۱(۴) (اختیاری)	شکست در رمزنگاری درهم‌سازی برای صحت داده‌ها	حالت رمزنگاری عملیات، شناسه/ نام موجودیت غیرفعال در حال درهم‌سازی
تولید بیت تصادفی (اختیاری)	شکست در تولید بیت تصادفی	هیچ
الزامات پروتکل IPSEC (اختیاری)	شکست در برقراری نشست SA، برقراری /پایان یک نشست	ارتباط نقطه پایانی غیرمحصول (آدرس IP)، دلیل شکست (در صورت قابل اجرا بودن)
الزامات پروتکل SSH (اختیاری)	شکست در برقراری یک نشست، برقراری یا خاتمه نشست	ارتباط نقطه پایانی غیرمحصول (آدرس IP)، دلیل شکست (در صورت قابل اجرا بودن)
الزامات پروتکل TLS (اختیاری)	شکست در برقراری یک نشست، برقراری یا خاتمه نشست	ارتباط نقطه پایانی غیرمحصول (آدرس IP)، دلیل شکست (در صورت قابل اجرا بودن)
خط‌مشی کنترل دسترسی ۱	هر تغییری در خط‌مشی‌های اعمال‌شده	شناسایی سامانه مدیریت خط‌مشی که تغییرات را ایجاد کرده است
عملیات کنترل دسترسی	تمام درخواست‌ها برای اجرای یک عملیات بر روی موجودیت غیرفعال که توسط محصول پوشش داده‌شده است	شناسایی موجودیت فعال، شناسایی موجودیت غیرفعال، عملیات درخواست شده
مدیریت کارکرد در محصول ۱	تمام تغییرات در رفتار محصول	هیچ
حفظ وضعیت امن در زمان شکست ۲	شکست در ارتباط بین محصول و مدیریت خط‌مشی (کلاینت)	شناسایی سامانه مدیریت خط‌مشی، دلیل شکست

[1] Mode

تشخیص تکرار	تشخیص تکرار	اقداماتی باید براساس عملیات اتخاذ گردد
برقراری نشست ۱ (اختیاری)	انکار از آغاز نشست	هیچ
کانال مطمئن	تمامی کاربردها از توابع کانال مطمئن	شناسایی آغازکننده و مقصد در کانال مطمئن

۲ **تولید داده ممیزی امنیت (۲)**

محصول باید برای هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید:

- تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال (در صورتی که کاربرد داشته باشد) و نتیجه (موفقیت یا شکست) رویداد
- [اختصاص: ممیزی دیگر اطلاعات مرتبط]

نکته کاربردی ۱:

در قسمت اختصاص عبارت «ممیزی دیگر اطلاعات مرتبط» باید شامل اطلاعات کافی برای شناسایی افراد مسئول و عملیات مشخصی که توسط آن‌ها انجام می‌گیرد، باشد.

۳ **ممیزی انتخابی ۱**

محصول باید قابلیت انتخاب رویدادهای قابل ممیزی بر اساس دارا بودن/ نبودن مشخصه‌های زیر از مجموعه رویدادهای ممیزی را داشته باشند:

الف-[انتخاب: هویت موجودیت غیرفعال، هویت کاربر، هویت موجودیت فعال، هویت میزبان، نوع رویداد]

ب -[اختصاص: فهرستی از مشخصه‌های تکمیلی که انتخاب ممیزی بر اساس آن می‌باشد].

نکته کاربردی ۲:

	قابلیت ممیزی انتخابی انتظار می‌رود توسط مدیریت خط‌مشی یا مدیریت پیکربندی امن اجرا شود، نه از طریق دسترسی مستقیم کاربر به محصول.
۴	**ذخیره‌سازی رویدادهای ممیزی ۱**
	محصول باید از رویدادهای ممیزی ذخیره‌شده در محل ذخیره‌سازی در برابر حذف غیر مجاز محافظت نماید.
۵	**ذخیره‌سازی رویدادهای ممیزی ۲**
	محصول باید قادر به تشخیص تغییرات غیرمجاز در رکوردهای ممیزی ذخیره‌شده در محل ذخیره‌سازی آن‌ها باشد. **نکته کاربردی ۳:** محصول برای خارج کردن اطلاعات ممیزی نیاز به مقداری حافظه در محل ذخیره‌سازی محلی دارد. نویسنده سند هدف امنیتی باید مقدار حافظه محلی را با مگابایت، متوسط تعداد رکوردهای ممیزی را نیز مشخص نماید.
۶	**ذخیره‌سازی رویدادهای ممیزی خارجی ۱**

محصول باید قادر به انتقال داده ممیزی تولیدشده به [اختصاص: لیستی از موجودیت‌های IT خارجی و/یا «محل ذخیره‌سازی در داخل محصول»] باشد. **نکته کاربردی ۴:** اصطلاح انتقال به هر دو فاز «آغاز محصول» برای انتقال اطلاعات و همچنین اطلاعات انتقالی محصول در واکنش به درخواست یک موجودیت IT خارجی اشاره دارد. نمونه‌هایی از موجودیت‌های خارجی می‌توان به سرور ممیزی بر روی یک ماشین خارجی، یک سیستم‌عامل ارزیابی‌شده که با محصول پلتفرمی را به اشتراک گذارده می‌توان اشاره نمود.	
۷	**ذخیره‌سازی رویدادهای ممیزی خارجی ۲**
محصول باید اطمینان دهد که برای انتقال داده ممیزی تولیدشده به هر موجودیت IT خارجی از یک کانال امن تعریف‌شده در شماره الزام ۳۹ «کانال مطمئن ۱» استفاده می‌نماید.	
۸	**ذخیره‌سازی رویدادهای ممیزی خارجی ۳**
محصول باید اطمینان دهد که محل ذخیره‌سازی داخلی محصول از هر داده ممیزی تولیدشده: • رکوردهای ممیزی ذخیره‌شده در دنباله ممیزی داخلی محصول را از حذف غیرمجاز محافظت می‌نماید و • از تغییرات غیرمجاز در رکوردهای ممیزی ذخیره‌شده در دنباله ممیزی داخل محصول جلوگیری می‌نماید. **نکته کاربردی ۵:** این الزام قابلیت محافظت از داده‌های ممیزی تولیدشده هنگام انتقال به یک یا چند موجودیت IT خارجی را فراهم می‌کند، همچنین از ذخیره‌سازی محلی و محافظت از داده‌های ممیزی تولیدشده را پشتیبانی می‌نماید (به عنوان مثال، هنگام ارتباط با موجودیت IT خارجی به طور موقت دسترسی قطع گردد). نویسنده هدف امنیتی باید نحوه ثبت رکورد ممیزی هنگام قطع ارتباط با موجودیت IT خارجی را بیان نماید و همچنین نحوه سنکرون شدن آن‌ها بعد از آغاز ارتباط مجدد را توضیح دهد.	

۲,۶ کلاس ارتباطات

شماره الزام	نام الزام
۹	**عدم انکار اطلاعات توسط گیرنده ۴**
محصول باید برای تمام خط‌مشی‌هایی که در هر زمانی دریافت می‌نماید، رسید[۱] دریافت تولید نماید.	
۱۰	**عدم انکار اطلاعات توسط گیرنده ۵**
محصول باید قادر به مرتبط نمودن [اختصاص: لیستی از مشخصه‌ها] از دریافت‌کننده اطلاعات و [اختصاص: لیستی از فیلدهای اطلاعاتی] از اطلاعات به رسید دریافتی باشد. **نکته کاربردی ۶:** نویسنده سند هدف امنیتی باید اختصاص اول را با اطلاعاتی تکمیل نماید که محصول برای شناساندن خود به عنوان دریافت‌کننده معتبر خط‌مشی استفاده می‌نماید (همچون نام میزبان، آدرس IP، آدرس و گواهی دیجیتال) نویسنده سند هدف امنیتی باید اختصاص دوم را با اطلاعاتی تکمیل نماید که به عنوان شناسه منحصر به فرد یک خط‌مشی استفاده می‌شود (همچون نام خط‌مشی و نسخه) طوری که بتوان این رسید را برای محصول مدیریت خط‌مشی ارسال نمود.	
۱۱	**عدم انکار اطلاعات توسط گیرنده ۶**

[۱] Evidance

محصول باید امکان بررسی رسید دریافت اطلاعات را به فرستنده در [اختصاص: محدودیت بر روی رسید دریافت] معین‌شده، فراهم نماید.

نکته کاربردی ۷:

نویسنده سند هدف امنیتی باید اختصاص را با مدت زمان کامل نماید که محصول خط‌مشی دریافتی و وضعیت اجرای آن را برای محصول مدیریت خط-مشی ارسال می‌نماید.

۳٫۶ کلاس پشتیبانی از رمزنگاری

الزامات رمزنگاری ممکن است هم از طریق محصول و یا توسط مؤلفه‌های محیط عملیاتی پیاده‌سازی گردد؛ اما انتظار می‌رود، محصول باید قادر به استفاده از الگوریتم‌های رمزنگاری که معتبر هستند باشد. نویسنده سند هدف امنیتی باید به‌طور واضح نشان دهد که چه الگوریتم‌هایی توسط محصول استفاده می-شود. در این صورت نویسنده هدف امنیتی باید در «پیوست یک» این الزامات نیز تکمیل نمایند.

در این کلاس الزامات توسعه‌یافته‌ای بر روی پروتکل‌های IPSEC، TLS، HTTPs و SSH در پیوست تعریف‌شده است. نویسنده سند هدف امنیتی در صورت به‌کاربرده شدن این پروتکل‌ها در سامانه باید از «الزامات پیوست یک» استفاده نماید.

۴٫۶ کلاس حفاظت از داده کاربری

در این پروفایل حفاظتی سه نوع سازوکار محافظت از داده معرفی‌شده است که با توجه به موقعیت‌های مختلف استفاده از کنترل دسترسی ضروری است. لیست چنین سازوکارهایی انتظار می‌رود با گذشت زمان اصلاح گردد تا امکانات اضافی کنترل دسترسی نیز ضروری شوند.

در حال حاضر سه مجموعه متفاوتی از الزامات «خط‌مشی کنترل دسترسی» و «عملیات کنترل دسترسی» در این پروفایل حفاظتی وجود دارد. وابسته به نوع سازوکار حفاظت از داده‌ها که در محصول بکار گرفته می‌شوند باید نویسنده سند هدف امنیتی الزامات را انتخاب نماید. این الزامات در «پیوست دو» قرار دارد. سه سازوکار فعلی که می‌توانند در محصول بکار گرفته شوند به شرح زیر است:

کنترل دسترسی مبتنی بر میزبان، کنترل دسترسی مبتنی بر شبکه و کنترل دسترسی جلوگیری از نشت داده‌ها.

شماره الزام	نام الزام
۱۲	**خط‌مشی کنترل دسترسی ۱**
به «پیوست دو» مراجعه کنید. **نکته کاربردی ۸:** اگر محصول قادر به استفاده از چندین نوع سازوکار کنترل دسترسی همزمان باشد (مبتنی بر میزبان، جلوگیری از نشت داده‌ها و غیره)، ضروری است که الزام برای هر نوع خط‌مشی تکرار شود. در این صورت تغییر نام خط‌مشی‌های مورد اعمال‌شده مورد قبول است تا ابهامی در اصطلاح کنترل دسترسی محصول ایجاد نشود. به عنوان مثال، نام الزام می‌تواند به صورت «خط‌مشی کنترل دسترسی ۱ (۱)- مبتنی بر میزبان» و «خط‌مشی کنترل دسترسی ۱ (۲)- جلوگیری از نشت داده‌ها» تغییر کند.	
۱۳	عملیات **کنترل دسترسی ۱**
به «پیوست دو» مراجعه کنید. **نکته کاربردی ۹:** اگر محصول قادر به استفاده از چندین نوع سازوکار کنترل دسترسی همزمان باشد (مبتنی بر میزبان، جلوگیری از نشت داده‌ها و غیره)، ضروری است که الزام برای هر نوع خط‌مشی تکرار شود. در این صورت تغییر نام خط‌مشی‌های مورد اعمال‌شده مورد قبول است تا ابهامی در اصطلاح کنترل دسترسی محصول ایجاد نشود. به عنوان مثال، نام الزام می‌تواند به صورت «خط‌مشی کنترل دسترسی ۱ (۱)- مبتنی بر میزبان» و «خط‌مشی کنترل دسترسی ۱ (۲)- جلوگیری از نشت داده‌ها» تغییر کند.	

۵,۶ کلاس شناسایی و احراز هویت

شماره الزام	نام الزام

۱۴	**مدیریت احراز هویت ناموفق ۱**

محصول، باید بتواند با استفاده از [انتخاب: [اختصاص: یک عدد مثبت]، یک عدد مثبت قابل تنظیم توسط مدیر [اختصاص: بازه قابل قبولی از مقادیر]] تلاش ناموفق احراز هویت مرتبط با [اختصاص: لیستی از رویدادهای احراز هویت] را تشخیص دهد.

نکته کاربردی ۱۰:

- محصول ممکن است برای کاربران مختلف، متدهای احراز هویت متفاوتی استفاده کند و از قوانین مختلفی براساس متدهای احراز هویت /یا کاربران جهت مدیریت کردن احراز هویت ناموفق بهره بگیرد. رفتاری که در قبال احراز هویت ناموفق، برای سیستم‌های از راه دور و کاربران انسانی صورت می‌گیرد، معمولان متفاوت از هم می‌باشد.

حتی برای کاربران انسانی ممکن است، عکس‌العمل در برابر احراز هویت ناموفق برای احراز هویتی که از طریق نام کاربری/رمز عبور صورت می‌گیرد نسبت به احراز هویتی که از طریق کارت هوشمند یا گواهینامه‌های دیجیتال انجام می‌گیرد، متفاوت باشد.

- رویداد احراز هویت ناموفق با توجه به آخرین نشست موفق در ترمینال شمارش می‌شود.
- هرچند که لیستی از اقدامات می‌تواند توسط محصول، مشخص شود.اما این مجموعه اقدامات باید اطمینان دهد که از حملات مبتنی بر جستجو در فضاهای ممکن جلوگیری می‌کند.

۱۵	**مدیریت احراز هویت ناموفق ۲**

زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت [انتخاب: به حد تعیین‌شده رسید و یا از آن بیشتر شد]، محصول باید [اختصاص: لیستی از اقدامات مقابله‌ای] را اجرا نماید که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود.

نکته کاربردی ۱۱:

از آنجا که نیازی به قفل نمودن حساب کاربری سرپرست دیده نمی‌شود، این الزام برای سرپرستان محلی به‌کاربرده نمی‌شود، بدین منظور حساب کاربری سرپرست محلی از سایر حساب‌های کاربری مجزا می‌گردد، جداسازی حساب کاربری سرپرست از کاربران می‌تواند در سند مربوط به سرپرست بیان گردد یا سازوکار احراز هویت محصول، می‌تواند تلاش‌های ورود محلی به سیستم را از تلاش‌های ورود از راه دور به سیستم متمایز نماید.

۱۶	**احراز هویت کاربر ۱**

محصول، باید اجازه انجام [اختصاص: **لیستی از اقدامات میانی**] پیش از احراز هویت را به کاربر بدهند. **نکته کاربردی ۱۲:** نویسنده سند هدف امنیتی باید هرگونه اقدام میانی که مجاز است پیش از احراز هویت کاربر انجام بگیرد را مشخص نماید. این اقدامات باید کاربر را به صورت محدودی در دستیابی به محصول کمک نماید. از اقدامات قابل قبول، قبل از احراز هویت کاربر استفاده از امکانات راهنما است.	
۱۷	**احراز هویت کاربر۲**
محصول، باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری از سوی او وجود داشته باشد، با موفقیت احراز هویت نمایند.	
۱۸	**احراز هویت کاربر۱۰**
محصول باید در حین پروسه احراز هویت [اختصاص: لیستی از بازخوردها] به کاربر ارائه دهد. **نکته کاربردی ۱۳:** از جمله باز خوردها می‌توان به *اشاره نمود که در هنگام وارد نمودن رمز عبور توسط کاربر، کاراکترها به صورت * نمایش داده می‌شوند.	
۱۹	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱**
محصول باید [اختصاص: لیستی از مشخصه‌های امنیتی کاربر] را با اقداماتی که از سوی کاربر انجام می‌شود، ارتباط دهند.	
۲۰	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲**
محصول باید [اختصاص: قوانین مرتبط با ارتباط اولیه‌ی مشخصه‌های امنیتی]کاربر با موجودیت‌های فعالی که از سوی کاربر انجام می‌شود، اعمال نماید.	
۲۱	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳**
محصول باید مشخصه‌های امنیتی کاربر که با موجودیت‌های فعال تحت استفاده کاربر مرتبط شده‌اند، [اختصاص: قوانین حاکم بر تغییرات مشخصه‌ها]را اعمال نماید.	

۶,۶ کلاس مدیریت امنیت

شماره الزام	نام الزام
۲۲	**مدیریت کارکرد در محصول ۱ (۱)**
	محصول باید توانایی [انتخاب: تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار] کارکرد [انتخاب: رویدادهای ممیزی شده، کنترل دسترسی محصول، محل ذخیره‌سازی مورد اطمینان، خط‌مشی پیاده‌سازی شده محصول، اجرای کنترل دسترسی محصول در رویدادهای قطع ارتباطات، [اختصاص: **لیستی از دیگر کارکردها**] به [اختصاص: محصول مدیریت خط‌مشی مجاز و معتبر، **نقش‌های تعریف‌شده مجاز**] محدود نماید. **نکته کاربردی ۱۴:** نویسنده سند هدف امنیتی باید نحوه اطمینان محصول از محصول مدیریت خط‌مشی را باید تعریف نماید. برای مثال، ممکن است که از کلیدهایی بین دو محصول استفاده شود یا از طریق پرس‌وجوی نسخه محصول خارجی این اطمینان حاصل شود. لازم است که در «خلاصه شرح محصول» ذکر شود. محصول باید قابلیت تغییر رفتار جمع‌آوری داده‌های سیستم، آنالیز و عکس‌العمل را تنها به سرپرستان مجاز سیستم محدود نمایند.
۲۳	**مدیریت کارکرد در محصول ۱ (۲)**
	محصول باید توانایی [انتخاب: تعیین رفتار] کارکرد: [انتخاب: خط‌مشی استفاده‌شده توسط محصول، [اختصاص: دیگر کارکردها]] را به [اختصاص: یک سامانه‌ی مدیریت امنیت مجاز و سازگار] محدود نماید.
۲۴	**مدیریت مشخصه‌های امنیتی ۱**
	محصول باید [اختصاص: خط‌مشی‌های کنترل دسترسی] اعمال نماید تا توانایی [انتخاب: تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، [اختصاص: دیگر کارکردها]] مشخصه‌های امنیتی [خط‌مشی‌های کنترل دسترسی، مشخصه‌های کنترل دسترسی، وضعیت اجرای خط‌مشی کنترل دسترسی] به [انتخاب: محصول مدیریت خط‌مشی، نقش‌های تعریف‌شده مجاز] محدود نماید.
۲۵	**مدیریت مشخصه‌های امنیتی ۳**
	محصول باید [خط‌مشی‌های کنترل دسترسی] را ملزم به ارائه دادن مقادیر پیش‌فرض محدود برای مشخصه‌های امنیتی که در اجرای خط‌مشی‌های

کارکرد امنیتی استفاده می‌شوند، نماید. **نکته کاربردی ۱۵:** محصول باید لیست کنترل دسترسی را ملزم به ارائه دادن مقادیر پیش‌فرض مجاز برای مشخصه‌های امنیتی نماید که در اجرای خط‌مشی‌های کارکرد امنیتی استفاده می‌شوند.	
۲۶	**مدیریت مشخصه‌های امنیتی ۴**
محصول باید به [سامانه مدیریت خط‌مشی] اجازه مشخص نمودن مقادیر اولیه پیشنهادی دهد تا زمانی که یک اطلاعات یا موجودیت غیرفعال ایجاد می‌گردد، جایگزین مقادیر پیش‌فرض گردد. **نکته کاربردی ۱۶:** هدف از این الزام آن است که به طور پیش فرض، محصول مانع جایگزینی مقادیر شود و همچنین قابلیت اجازه عملیات از طریق اعمال تغییرات در پیکربندی محصول باشد.	
۲۷	**کارکرد مدیریتی محصول ۱**
محصول باید قادر به انجام کارکردهای مدیریتی [انتخاب: پیکربندی رویدادهای ممیزی، پیکربندی انباره برای ذخیره‌سازی ممیزی امن، پیکربندی کنترل دسترسی محصول، پرس‌وجوی خط‌مشی اجراشده توسط محصول، اعمال مدیریت رفتار کنترل دسترسی در رویدادهای قطع ارتباطات [اختصاص: دیگر کارکردهای مدیریتی محصول]] باشد.	
۲۸	**نقش‌های امنیتی ۱**
محصول، باید نقش‌های زیر را نگهداری نمایند: [اختصاص: **نقش‌های مجاز معرفی‌شده و مرتبط با محصولات مدیریت خط‌مشی که به محض آغاز اتصال با محصول کار می‌کنند]**	
۲۹	**نقش‌های امنیتی ۲**
محصول باید قادر به مرتبط نمودن کاربران با نقش‌هایشان باشند.	

۳۰	**مدیریت داده‌های محصول ۱**
محصول باید توانایی [انتخاب: تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن، [اختصاص: دیگر کارکردها]] [اختصاص: لیستی از داده‌های احراز هویت] را به [اختصاص: نقش‌های تعریف‌شده مجاز] محدود نماید. **نکته کاربردی ۱۷:** داده‌های احراز هویت می‌تواند در انباره خارج از محصول ذخیره شود. برای مثال، محصول ممکن است تغییرات کلمه عبور کاربر را در محیط عملیاتی سرور LDAP ذخیره نماید.	

۷,۶ کلاس حفاظت از محصول

شماره الزام	**نام الزام**
۳۱	**مهرهای زمانی ۱**
محصول باید قادر باشد برای استفاده خودش مهرهای زمانی قابل اطمینانی ارائه دهد.	
۳۲	**حفاظت از کلمه عبور سرپرست ۱**
محصول باید کلمه‌های عبور را به صورت متن آشکار ذخیره ننمایند.	
۳۳	**حفاظت از کلمه عبور سرپرست ۲**
محصول باید از خواندن متن آشکار اعتبارات جلوگیری نماید. **نکته کاربردی ۱۸:** منظور این الزام آن است که داده‌های مربوط به احراز هویت همچون کلمه عبور به صورت آشکار ذخیره نشوند و هیچ کاربری یا سرپرستی قادر به خواندن کلمه عبورهای آشکار از طریق واسط‌های معمولی نباشد.	
۳۴	**حفظ وضعیت امن در زمان شکست ۲**
محصول باید در شرایطی که ارتباطش با سامانه مدیریت خط‌مشی با شکست مواجه شده، یکی از خط‌مشی‌های زیر را حفظ نماید: [انتخاب: انکار تمام درخواست‌ها، اعمال آخرین خط‌مشی دریافت شده، [اختصاص: خط‌مشی شکست]]	

نکته کاربردی ۱۹: نویسنده سند هدف امنیتی با تعریف مجدد این الزام می‌تواند رفتار محصول را در رویداد «شکست ارتباط محصول» و همچنین «مدیریت خط‌مشی با دیگر محصول» بیان نماید.	
۳۵	**تشخیص تکرار ۱**
محصول باید برای موجودیت‌های [اختصاص: لیستی از موجودیت‌های شناسایی‌شده] تکرار را تشخیص دهد. **نکته کاربردی ۲۰:** در قسمت اختصاص حتماً باید موجودیت شناسایی‌شده‌ای تعیین گردد.	
۳۶	**تشخیص تکرار ۲**
محصول باید در هنگام تشخیص تکرار [اختصاص: لیستی از اقدامات مشخص] را انجام دهد. **نکته کاربردی ۲۱:** در قسمت اختصاص حتماً باید اقدام خاصی تعیین گردد.	
۳۷	**محافظت از داده‌های محصول (کلیدهای متقارن) ۱**
محصول باید از خوانده شدن تمام کلیدهای از پیش به اشتراک گذارده شده، کلیدهای متقارن و کلیدهای خصوصی جلوگیری نمایند. **نکته کاربردی ۲۲:** منظور این الزام آن است که سرپرست قادر به مشاهده و خواندن کلیدهای شناسایی‌شده از طریق واسط‌های «معمول» نمی‌باشد واضح است که سرپرست می‌تواند مستقیماً حافظه را بخواند و یا کلیدها را مشاهده نماید، اما انجام این امر نیز به سادگی نمی‌باشد؛ بنابراین سرپرست به عنوان یک عامل امن در نظر گرفته می‌شود که سعی در خواندن یا مشاهده کلید ندارد.	

۸,۶ کلاس تخصیص منابع

شماره الزام	نام الزام

۳۸	**تحمل خطا ۱**
محصول باید در زمان رخداد شکست‌های زیر نسبت به اعمال خط‌مشی اطمینان دهد: برقراری ارتباط با سامانه مدیریت خط‌مشی پس از قطع برق	

۹,۶ کلاس‌ها مسیرها و کانال‌های امن

شماره الزام	نام الزام
۳۹	**کانال مطمئن ۱**
محصول باید از پروتکل‌های [انتخاب: IPsec, SSH, TLS, TLS/HTTP] استفاده نماید تا کانال ارتباطی امنی بین خود و موجودیت IT که به صورت منطقی از دیگر کانال‌های ارتباطی مجزا است برقرار نماید تا داده‌های کانال را از تغییر و افشاء محافظت نماید. **نکته کاربردی ۲۳:** منظور الزام بالا استفاده از پروتکل‌های رمزنگاری جهت حفاظت ارتباطات خارجی با موجودیت‌های IT مجازی است که محصول برای انجام کارکردهایش با آن‌ها در تعامل است. در این الزام نویسنده سند هدف امنیتی پروتکل‌های رمزنگاری یا پروتکل‌هایی برای جفاظت کانال ارتباطی را مشخص می‌نماید. سپس با توجه به پروتکل انتخابی الزام مناسب آن پروتکل را از پیوست انتخاب می‌نماید.	
۴۰	**کانال مطمئن ۲**
محصول باید [انتخاب: محصول، دیگر محصول IT امن] را مجاز نماید تا ارتباط را از طریق کانال امن آغاز نماید.	
۴۱	**کانال مطمئن ۳**
محصول باید برای انتقال داده خط‌مشی، [اختصاص: دیگر کارکردها] از طریق کانال امن ارتباط را آغاز نماید. **نکته کاربردی ۲۴:** نویسنده سند هدف امنیتی قسمت اختصاص را با تمام ارتباطات محافظت‌شده‌ای که محصول با دیگر بخش‌های سامانه مدیریت امنیت دارد، کامل می‌نماید	

(انتقال داده ممیزی، درخواست داده شناسایی و غیره.)	
۴۲	مسیر مطمئن ۱
محصول، باید مسیر ارتباطی امنی را با استفاده از [انتخاب: IPsec, SSH, TLS, HTTPS] برای ایجاد کانال ارتباطی امن بین خود و کاربران راه دور را داشته که به طور منطقی از سایر مسیرهای ارتباطی مجزا هستند را فراهم نماید تا نقاط پایانی خود را احراز هویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.	
۴۳	مسیر مطمئن ۲
محصول باید به کاربران راه دور معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.	
۴۴	مسیر مطمئن ۳
محصول باید از مسیر مطمئنی برای احراز هویت اولیه کاربر، اجرای توابع مدیریتی استفاده نماید.	

۱۰,۶ کلاس سامانه مدیریت امنیت

شماره الزام	نام الزام
۴۵	**شناسایی موجودیت غیرفعال ۱**
	محصول باید قادر به کشف و شناسایی موجودیت‌های غیرفعال در محیط عملیاتی با توجه به شرایط زیر باشد:[انتخاب: داده‌های رمزنگاری نشده که نیاز به خط‌مشی رمزنگاری دارند، داده‌هایی که در دامنه قرار دارند و با مشخصه‌های امنیتی داده‌های تعریف‌شده سازگاری ندارند، [اختصاص: دیگر شرایطی که نشانگر داده‌های مقیم در محیط عملیاتی هستند که باید توسط محصول فهرست شوند]]. **نکته کاربردی ۲۵:** هدف شناسایی موجودیت غیرفعال محصول در پروفایل حفاظتی به این دلیل است که برای خروج داده‌هایی که در دامنه مقیم هستند، باید اجازه صادر شود.
۴۶	**شناسایی موجودیت غیرفعال ۲**
	محصول باید اقدامات زیر را برای کشف و شناسایی موجودیت غیرفعال تعریف‌شده در الزام شماره ۴۲«شناسایی موجودیت غیرفعال ۱» انجام دهد: [انتخاب: رمزنگاری موجودیت غیرفعال، انتقال موجودیت غیرفعال به یک مکان سازگار با مشخصه‌های حساس خود، حذف موجودیت غیرفعال، [اختصاص: دیگر اقدامات]].
۴۷	**شناسایی موجودیت فعال ۱**
	محصول باید برای شناسایی موجودیت فعال به [انتخاب: [اختصاص: مؤلفه‌های شناخته‌شده محصول که مسئول شناسایی موجودیت فعال]، [اختصاص: مؤلفه‌های محیط عملیاتی شناخته‌شده که مسئول شناسایی موجودیت فعال است]] تکیه نماید. **نکته کاربردی ۲۵:** اگر منظور از موجودیت فعال در این الزام کاربران یا مدیران می‌باشد، انتظار می‌رود قسمت اختصاص با یک یا بیش از یک سرور احراز هویت کامل گردد.
۴۸	**شناسایی موجودیت فعال ۲**
	محصول باید هر موجودیت فعال را ملزم نماید تا پیش از آنکه به هر اقدام میانی دیگری از سوی موجودیت فعال اجازه داده شود، به صورت موفقیت‌آمیزی شناسایی شود.

۴۹	**تعریف مشخصات موجودیت غیرفعال ۱**
	محصول باید [اختصاص: لیستی از مشخصه‌های امنیتی موجودیت‌های غیرفعال] را برای موجودیت‌های غیرفعال منحصربه فرد نگهداری نماید. **نکته کاربردی ۲۶:** به مشخصه‌های امنیتی موجودیت غیرفعال اشاره دارد که ممکن است در نهایت فاکتوری برای تصمیم کنترل دسترسی باشد اما با کاربر و یا خط‌مشی کنترل دسترسی مرتبط نیستند. محصول که خط‌مشی‌های کنترل دسترسی را برای امنیت چند سطحی تعریف می‌کند، ممکن است به تعیین برچسب‌های امنیتی نیاز داشته باشد تا بتواند با منابع (به منظور اینکه خط‌مشی در آن منابع قابل استفاده باشد) مرتبط شود.
۵۰	**تعریف مشخصات موجودیت غیرفعال ۲**
	محصول باید قادر به ایجاد ارتباط بین مشخصه‌های امنیتی با موجودیت‌های غیرفعال منحصربه‌فرد باشد.
۵۱	**شناسایی کاربر و موجودیت امن ۱**
	محصول باید بر [انتخاب: [اختصاص: مؤلفه‌های محصول که مسئول احراز هویت موجودیت فعال است]، [اختصاص: مؤلفه‌های محیط عملیاتی مشخص که مسئول احراز هویت موجودیت فعال است]] برای احراز هویت موجودیت فعال متکی باشد. **نکته کاربردی ۲۷:** اگر موجودیت فعال شناخته‌شده به عنوان کاربران یا مدیران محصول باشد، انتظار می‌رود که «اختصاص‌ها» با یک یا چند سرور احراز هویت کامل شوند.
۵۲	**شناسایی کاربر و موجودیت امن ۱**
	محصول باید تضمین نماید که هر موجودیت فعال قبل از احراز هویت موفق امکان اقدامات میانی را نداشته باشد. **نکته کاربردی ۲۸:** اگر محصول از دو متد مختلف برای احراز هویت دو مجموعه متفاوت از موجودیت‌های فعال استفاده نماید، نویسنده هدف امنیتی باید این موضوع را با ایجاد تکرارهای مختلف برای این الزام نمایش دهد.
۵۳	**تعریف مشخصات کاربر در محیط عملیاتی ۱**
	محصول باید توانایی تعریف مشخصات هویتی و داده‌های اعتبارنامه[1] را در دیگر محصولات سامانه مدیریت امنیت فراهم آورد.

[1] Credential data

نکته کاربردی ۲۹: مشخصه‌های اعتبارنامه و شناسایی مربوط به امنیت باید مجموعه کاملی از مشخصه‌های کاربر را که دیگر محصولات مدیریت امنیت سازمان برای اعمال کارکردهای امنیتی بکار می‌برند انتخاب کند. داده‌هایی مانند شناسه کاربر و کلمه عبور امنیتی هستند زیرا برای احراز هویت بکار می‌روند. داده‌هایی مانند نقش سازمانی کاربر، عنوان یا مکان جغرافیایی در صورتی که در خط‌مشی کنترل دسترسی مورد استفاده قرار گیرند، ممکن است به عنوان داده‌های امنیتی محسوب شوند. داده‌های از قبیل شماره تلفن به عنوان داده‌های امنیتی به حساب نمی‌آیند.	
۵۴	**تعریف مشخصات کاربر در محیط عملیاتی ۲**
محصول باید مشخصه‌های شناسایی و اعتبارنامه مرتبط با امنیت زیر را برای کاربران سازمان تعریف کند: طول عمر اعتبارنامه، وضعیت اعتبارنامه، [اختصاص: لیستی از مشخصه‌های شناسایی و اعتبارنامه امنیتی که محصول قادر به مرتبط ساختن آن‌ها با کاربران سازمان است.]	
۵۵	**تعریف مشخصات کاربر در محیط عملیاتی ۳**
محصول باید توانایی ثبت کردن کاربران سازمان را از طریق تخصیص داده‌های شناسایی منحصربه‌فرد ایجاد نماید. **نکته کاربردی ۳۰:** ممکن است که دو کاربر بتوانند داده‌های اعتبارنامه‌ای یکسانی داشته باشند. هدف از این الزام این است که اطلاعات اضافه‌تری نگهداری شود تا به‌طور منحصربه‌فرد کاربران خاص سازمان را شناسایی نماید.	
۵۶	**تعریف مشخصات کاربر در محیط عملیاتی ۴**
محصول باید توانایی مرتبط کردن مشخصه‌های امنیتی تعریف‌شده با کاربران ثبت‌شده را ایجاد کند.	
۵۷	**تعریف مشخصات کاربر در محیط عملیاتی ۵**
محصول باید توانایی پرس‌وجو کردن وضعیت اعتبارنامه‌های کاربران سازمان را ایجاد نماید.	
۵۸	**تعریف مشخصات کاربر در محیط عملیاتی ۶**
محصول باید توانایی لغو اعتبارنامه‌های کاربران سازمان را ایجاد کند.	
۵۹	**تعریف مشخصات کاربر در محیط عملیاتی ۷**

محصول باید برای محصول سرور احراز هویت مدیریت امنیت سازمان توانایی به‌روزرسانی اعتبارنامه‌های کاربران سازمان را ایجاد نماید.	
۶۰	**تعریف مشخصات کاربر در محیط عملیاتی ۸**
محصول باید اطمینان حاصل نماید که اعتبارنامه‌های تعریف‌شده کاربران سازمان قوانین زیر را برآورده نماید: الف) برای اعتبارنامه‌های مبتنی بر کلمه عبور قوانین زیر بکار می‌روند: ۱. کلمه عبورها باید از زیر مجموعه‌ای از مجموعه کارکترهای [اختصاص: لیستی از مجموعه کارکترهایی که توسط سیستم برای وارد کردن کلمه عبور پشتیبانی می‌شود] استفاده کند که شامل مقادیر [اختصاص: لیستی از کارکترهای پشتیبانی شده برای هر مجموعه کارکتر پشتیبانی شده] باشد. ۲. حداقل طول کلمه عبور باید توسط مدیر سیستم قابل پیکربندی بوده و حداقل ۱۵ یا بزرگ‌تر باشد. ۳. قوانین ترکیب کلمه عبور انواع و تعداد کارکترهای لازم را مشخص می‌کند که شامل کلمه عبوری است که توسط مدیر سیستم باید قابل پیکربندی باشد. ۴. آخرین کلمه عبورهای تعیین‌شده توسط مدیر سیستم نباید مجددا قابل استفاده باشد. ب) برای اعتبارنامه‌هایی که مبتنی بر کلمه عبور نیستند، قوانین زیر بکار می‌رود: ۱. احتمال این‌که یک راز توسط حمله‌کننده در طول عمر آن راز بدست آید کمتر از 2^{-20} است.	
۶۱	**انتقال داده‌های امنیتی کاربر به موجودیت امن ۱**
محصول باید [انتخاب: داده‌های شناسایی و اعتبارنامه، داده‌های شناسایی، اعتبارنامه‌ها و مشخصه‌های موجودیت غیرفعال] به محصولات مدیریت امنیت سازمانی مجاز و سازگار تحت شرایط زیر انتقال دهد: [انتخاب: یک یا چند موارد زیر انتخاب شود: داده‌ها سریعاً در محدوده‌ای متناوب، در لحظه درخواست محصول، [اختصاص: دیگر شرایط] ایجاد یا تصحیح شوند.]	

۱۱,۶ کلاس دسترسی به محصول

شماره الزام	نام الزام
۶۲	**قفل‌کردن و خاتمه دادن به نشست‌ها ۵**
محصول باید کلیه نشست‌های تعاملی راه دور[1] را پس از مدت زمان [اختصاص: **بازه زمانی که توسط مدیر تنظیم می‌شود**] غیرفعال بودن، خاتمه دهد.	
۶۳	**قفل‌کردن و خاتمه دادن به نشست‌ها ۶**
محصول باید به شروع‌کننده نشست، اجازه اتمام نشست تعاملی خودش را بدهد.	
۶۴	**پیغام‌های هشدار در رابطه با استفاده محصول ۱**
قبل از ایجاد نشست برای کاربر، محصول مورد ارزیابی باید پیام‌های هشدار توصیه‌های پیکربندی را بدون در نظر گرفتن استفاده غیرمجاز از محصول را به کاربر نشان دهد. **نکته کاربردی ۳۱:** این الزام در مورد نشست‌های تعاملی بین یک کاربر انسانی و یک محصول مورد ارزیابی اعمال می‌شود. موجودیت‌های IT که اتصالاتی مانند تماس‌های راه دور از طریق شبکه را برقرار می‌کنند، نیازی به رعایت این الزام نخواهند داشت.	
۶۵	**برقراری نشست ۱**
محصول باید قادر به جلوگیری از ایجاد نشست براساس [انتخاب: روز، زمان، [اختصاص: دیگر مشخصه‌ها]] باشد.	
۶۶	**قفل‌کردن و خاتمه دادن به نشست‌ها ۷**

[1] Remote

در مورد نشست‌های تعاملی محلی[1]، محصول مورد ارزیابی باید پس از اتمام زمان غیرفعال بودن که توسط مدیر سیستم تعیین‌شده است، [انتخاب:

- نشست را قفل کند – تمام فعالیت‌های مربوط به دسترسی به داده‌های کاربری و نمایش این داده‌ها، به‌جز فعالیت‌های مربوط به قفل‌گشایی نشست را غیرفعال کند و از کاربر بخواهد که پیش از قفل‌گشایی نشست، مجدداً احراز هویت نماید؛
- شست را خاتمه دهد].

[1] local

۷ الزامات تضمین امنیت

اهداف امنیتی تعریف‌شده در بخش ۴ جهت مقابله نمودن با تهدیدات معرفی‌شده در بخش ۳ در نظر گرفته‌شده‌اند. الزامات کارکردی در بخش ۵ بیان رسمی و استانداردی از «اهداف امنیتی» می‌باشد. الزامات تضمین امنیتی که برگرفته از استاندارد ارزیابی امنیتی معیار مشترک می‌باشند تا براساس این الزامات ارزیابی، مستندات را ارزیابی و آزمون مستقل برروی محصول انجام دهد.

مدل کلی ارزیابی محصول در برابر سند هدف امنیتی که مطابق این پروفایل حفاظتی است، به صورت زیر می‌باشد:

پس از تائید سند هدف امنیتی برای ارزیابی، تولیدکننده محصول رادر اختیار آزمایشگاه قرار می‌دهد و محیط آزمون آن را فراهم می‌نماید؛ و سپس فعالیت‌های تضمین که در سند هدف امنیتی مطرح‌شده، توسط آزمایشگاه انجام می‌شود. نتایج این فعالیت‌ها مستند و برای اعتباربخشی به مرکز گواهی ارائه می‌شود.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب‌گذاری هدف ارزیابی
	ALC_CMS.1	پوشش پیکربندی هدف ارزیابی

۱٫۷ کلاس توسعه

اطلاعات محصول، از طریق «مستندات راهنمای کاربر» و بخش «مشخصات امنیتی هدف ارزیابی» از سند هدف امنیتی در اختیار کاربر نهایی قرار می‌گیرد. الزامی بر وجود بخش «مشخصات امنیتی هدف ارزیابی» در سند هدف امنیتی نمی‌باشد، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه‌دهندگان هدف ارزیابی باشد.

مشخصات کارکردی:

مشخصات کارکردی، واسط‌های کارکرد امنیتی هدف ارزیابی را توصیف می‌نماید اما نیازی به شرح مفصل و کاملی از این واسط‌ها نمی‌باشد. فعالیت‌های این خانواده باید بر روی شناخت واسط‌های معرفی‌شده در بخش «مشخصات امنیتی هدف ارزیابی» از سند هدف امنیتی و «مستندات راهنما» متمرکز گردد.

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید مشخصات کارکردی را ارائه نماید. **نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده-

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
	سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات هدف ارزیابی» سند هدف امنیتی ارائه‌شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات هدف ارزیابی» وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح‌شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی‌باشد.

مؤلفه‌های محتوایی

نام خانواده	عنصر امنیتی
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1C)** **شرح مؤلفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجراکننده کارکرد امنیتی[1] و پشتیبان کننده‌ی الزام کارکرد امنیتی[2] توصیف نماید. **نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2C)** **شرح مؤلفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجراکننده کارکرد امنیتی و پشتیبان

[1]-SFR-enforcing TSFI

[2]-SFR-supporting TSFI

مؤلفه‌های محتوایی

نام خانواده	عنصر امنیتی
	کننده‌ی الزام کارکرد امنیتی را مشخص نماید. **نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.3C)** **شرح مؤلفه:** مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید. **نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.4C)** **شرح مؤلفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌های کارکرد امنیتی در سند مشخصات کارکردی باشد.

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید. **نام عنصر: مشخصات کارکرد ابتدایی۱**

مؤلفه‌های اقدامات ارزیاب

نام خانواده **عنصر امنیتی**

شماره مؤلفه: (ADV_FSP.1.2E)

شرح مؤلفه:

ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می-باشند.

مستندات «مشخصات کارکردی» جهت پشتیبانی از ارزیابی الزامات کارکردی و اقدامات لازم در کلاس‌های «راهنما»، «آزمون» و «آسیب‌پذیری» ارائه‌شده است.

۲,۷ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل سرپرستی و نحوه بررسی محیط عملیاتی توسط سرپرست (تا مشخص گردد که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می‌شود.

برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد. این راهنما شامل:

دستورالعمل نصب موفقیت‌آمیز هدف ارزیابی در محیط

دستورالعمل مدیریت امنیت هدف ارزیابی به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگ‌تر

دستورالعمل‌هایی که ارائه‌دهنده قابلیت سرپرستی محافظت‌شده از طریق استفاده از قابلیت‌های هدف ارزیابی، محیط عملیاتی یا هر دو می‌باشد.

راهنمای کاربردی

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده **عنصر امنیتی**

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.

مؤلفه‌های محتوایی

نام خانواده	عنصر امنیتی
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب. **نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه‌شده توسط هدف ارزیابی به صورت امن استفاده می‌گردد. **نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.3C)**

مؤلفه‌های محتوایی

نام خانواده **عنصر امنیتی**

شرح مؤلفه:

سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های در دسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.

نام عنصر: راهنمای کاربردی ۱

شماره مؤلفه: (AGD_OPE.1.4C)

شرح مؤلفه:

سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی هدف ارزیابی.

نام عنصر: راهنمای کاربردی ۱

شماره مؤلفه: (AGD_OPE.1.5C)

شرح مؤلفه:

سند راهنمای کاربردی باید تمام مدهای عملیاتی هدف ارزیابی (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آن‌ها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.

نام عنصر: راهنمای کاربردی ۱

شماره مؤلفه: (AGD_OPE.1.6C)

شرح مؤلفه:

سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده‌شده‌اند، کاملاً اجرا

مؤلفه‌های محتوایی

نام خانواده	عنصر امنیتی
	گردند. **نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.7C)** **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱**

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده **عنصر امنیتی**

شماره مؤلفه: (AGD_PRE.1.1D)

شرح مؤلفه:

توسعه‌دهنده باید هدف ارزیابی را همراه با سند آماده‌سازی ارائه نماید.

مؤلفه‌های اقدامات محتوایی

نام خانواده **عنصر امنیتی**

راهنمای آماده‌سازی **(AGD_PRE)**

نام عنصر: راهنمای آماده‌سازی ۱

شماره مؤلفه: (AGD_PRE.1.1C)

شرح مؤلفه:

مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن هدف ارزیابی توسط مشتری را مطابق با رویه‌های تحویل توسعه‌دهنده شرح دهند.

نام عنصر: راهنمای آماده‌سازی ۱

شماره مؤلفه: (AGD_PRE.1.2C)

شرح مؤلفه:

مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن هدف ارزیابی و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکرشده در سند هدف امنیتی، شرح دهند.

مؤلفه‌های اقدامات ارزیاب

راهنمای آماده‌سازی **نام عنصر: راهنمای آماده‌سازی ۱**

مؤلفه‌های اقدامات ارزیاب (AGD_PRE)

شماره مؤلفه: (AGD_PRE.1.1E)

شرح مؤلفه:

ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

نام عنصر: راهنمای آماده‌سازی ۱

شماره مؤلفه: (AGD_PRE.1.2E)

شرح مؤلفه:

ارزیاب باید رویه‌های آماده‌سازی شرح داده‌شده در سند را بکار ببرد تا تائید نماید، هدف ارزیابی می‌تواند به صورت امن برای عمل نمودن آماده شود.

۳,۷ کلاس آزمون

آزمون محصول برای بررسی بخش‌های کارکردی سیستم و همچنین بخش‌هایی که طراحی و پیاده‌سازی آن‌ها برای سیستم دارای آسیب‌های امنیتی است، در نظر گرفته می‌شود. آزمون بخش‌های کارکردی سیستم از طریق خانواده ATE_IND؛ و آزمون بخش‌هایی که طراحی و پیاده‌سازی آسیب‌زایی دارند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) آزمون براساس کارکردی که برای هدف ارزیابی در نظر گرفته‌شده و واسط‌هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌گردد. نتایج آزمون و تحلیل آسیب‌پذیری باید در گزارش آزمون لحاظ شوند این مسئله در الزامات زیر در نظر گرفته‌شده است.

آزمون مستقل

«آزمون مستقل» برای تائید عملکرد محصول که در بخش «مشخصات امنیتی هدف ارزیابی» از سند هدف امنیتی و مستندات «راهنمای سرپرست» ارائه‌شده، صورت می‌گیرند. هدف اصلی آزمون اطمینان از برآورده شدن الزامات کارکردی مشخص‌شده در سند هدف امنیتی می‌باشد. ارزیاب باید در سند «گزارش آزمون»، طرح آزمون و نتایج آن را مستند نماید.

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
آزمون مستقل (ATE_IND)	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمودن، هدف ارزیابی را ارائه نماید.

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی
آزمون مستقل (ATE_IND)	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1C)** **شرح مؤلفه:** هدف ارزیابی باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب

آزمون مستقل (ATE_IND)	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، مؤلفه‌های محتوایی را برآورده می‌نماید. **نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.2E)**

مؤلفه‌های اقدامات ارزیاب

شرح مؤلفه:

ارزیاب باید زیرمجموعه‌ای از توابع امنیتی هدف ارزیابی را آزمون نماید تا تائید نماید که توابع امنیتی هدف ارزیابی به صورت مشخص‌شده عمل می‌نمایند.

۴,۷ کلاس آسیب‌پذیری

تحلیل آسیب‌پذیری

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمودن، هدف ارزیابی را ارائه نماید.

مؤلفه‌های اقدامات محتوایی

نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1C)** **شرح مؤلفه:**

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی
	هدف ارزیابی باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، تمام مؤلفه‌های محتوایی را برآورده می‌نماید. **نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.2E)** **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در هدف ارزیابی، در منابع عمومی جستجویی را انجام دهد. **نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.3E)** **شرح مؤلفه:** ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی‌شده، آزمون نفوذ انجام دهد تا مقاومت هدف ارزیابی را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۵٫۷ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه‌شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی‌هایی از چرخه حیات محدود می‌گردد که توسط کاربر نهایی قابل مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه‌دهنده نقش کمرنگی در قابل اعتماد بودن محصول دارد، بلکه در این سطح اطمینان (EAL1) تنها به این اطلاعات نیاز است.

قابلیت‌های پیکربندی

این مؤلفه جهت معرفی هدف ارزیابی به صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه‌شده، می‌باشد (بدین معنی که جدا از برچسب‌گذاری محصول، هدف ارزیابی که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب‌گذاری شود، نام هدف ارزیابی، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند هدف ارزیابی که توسط مرکز گواهی تائید شده است را به آسانی تشخیص دهد.

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMC.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید هدف ارزیابی و مرجع هدف ارزیابی را ارائه نماید.

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMC.1.1C)**

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی
	شرح مؤلفه: هدف ارزیابی باید با یک مرجع یکتا برچسب زده شود.

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMC.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

حوزه پیکربندی

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1D)** **شرح مؤلفه:** ارزیاب باید لیست پیکربندی هدف ارزیابی را ارائه نماید.

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** لیست پیکربندی باید شامل خود هدف ارزیابی و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد. **نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۸ پیوست یک: الزامات رمزنگاری توسعه‌یافته

در این قسمت خانواده‌های توسعه‌یافته‌ای از کلاس رمزنگاری تعریف‌شده‌اند. این خانواده‌ها مرتبط با پروتکل‌های IPsec، HTTPS، TLS و SSH می‌باشد. در صورت استفاده از چنین **پروتکل‌هایی و یا رمزنگاری کلیدها و اعتبارات**، نویسنده سند هدف امنیتی باید در کلاس رمزنگاری الزامات مرتبط با آن پروتکل را در نظر بگیرد.

شماره الزام	نام الزام
۶۷	**مدیریت کلید رمزنگاری ۱**
محصول باید کلیدهای رمزنگاری نامتقارن که برای ایجاد کلید استفاده می‌شوند را مطابق با استاندارد [انتخاب: • *استاندارد NIST SP 800-56 A، «توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری لگاریتمی گسسته» برای طرح برقراری کلید متناهی مبتنی بر میدان*[1] • *استاندارد NIST 800-56 A، «توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری لگاریتمی گسسته*[2]*» برای برقراری طرح کلید مبتنی بر منحنی بیضوی*[3] *و پیاده‌سازی «NIST Curves» در P-256 و P-384 و [گزینه P-521 و نه منحنی دیگری] (چنان‌که در FIPS PUB 186-3، «استاندارد امضای دیجیتال» تعریف‌شده است)* • *استاندارد NIST SP 800-56 B، «توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری تجزیه عدد صحیح*[4] *برای طرح برقراری کلید مبتنی بر RSA».*] تولید نمایند. همچنین اندازه‌ی این کلید باید معادل یا بزرگ‌تر از قدرت یک کلید متقارن ۱۱۲ بیتی باشد.	

[1] Field-bsae

[2] Discrete Logarithm Cryptography

[3] Curve-base

[4] Integer Factorization Cryptography

نکته کاربردی ۳۲:

این مؤلفه محصول را قادر می‌سازد تا برای پروتکل‌های مختلف رمزنگاری (برای مثال IPsec) که توسط محصول استفاده می‌گردند، جفت کلید عمومی/خصوصی تولید نمایند.

در صورتی که نویسنده سند هدف امنیتی بیش از یک مورد از موارد قسمت «انتخاب» را برگزیند، این الزام در سند هدف امنیتی برای هر یک از موارد انتخاب‌شده باید تکرار گردد.

قدرت کلید تولیدشده ۲۰۴۸ بیتی DSA و rDSA به قدرتی معادل یا بزرگ‌تر از قدرت یک کلید متقارن ۱۱۲ بیتی نیاز دارد. برای اطلاعات بیشتر در رابطه با قدرت کلید معادل به استاندارد NIST 800-57(«توصیه برای مدیریت کلید» مراجعه شود.

۶۸	**مدیریت کلید رمزنگاری ۶**

محصول باید براساس متد تخریب کلید رمزنگاری [اختصاص: **متد تخریب کلید رمزنگاری**] که بر اساس استاندارد [اختصاص: **لیستی از استانداردها**] باشد، کلیدهای رمزنگاری را از بین ببرد.

نکته کاربردی ۳۳:

هرگونه اطلاعات امنیتی (از قبیل کلیدها، داده‌های احراز هویت و کلمه عبورها) باید در صورت عدم استفاده به دلیل جلوگیری از افشای اطلاعات و یا ویرایش داده‌های امنیتی تخریب شوند.

۶۹	**عملیات رمزنگاری ۱(۱) – رمزنگاری و رمزگشایی**

محصول باید رمزنگاری و رمزگشایی را مطابق با الگوریتم رمزنگاری **AESکه در [اختصاص: یک یا چند مد] عمل می‌نماید** با کلید رمزنگاری با اندازه-های ۱۲۸ و ۲۵۶ بیتی و [انتخاب: *۱۹۲ بیتی، هیچ اندازه دیگری*] مطابق با استانداردهای زیر انجام بدهند:

- *استاندارد FIPS PUB 197*
- [انتخاب: *NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D, NIST SP 800-38E]*

نکته کاربردی ۳۴:

در قسمت «اختصاص» الگوریتم رمزنگاری، باید مد یا مدهایی که الگوریتم AES عمل می‌کند، الزام داده شود.

	در صورتی که الگوریتم AES از اندازه‌های دیگری به جز ۱۲۸ و ۲۵۶ بیت برای کلید استفاده نماید، در قسمت «انتخاب» مربوط به اندازه کلید، مقدار جدید انتخاب می‌گردد. در دومین «انتخاب» مربوط به مشخص نمودن استاندارد، استانداردهایی انتخاب می‌شوند که مدهای مشخص‌شده در بخش اختصاص را شرح می‌دهند.
۷۰	**عملیات رمزنگاری ۱(۲)- امضاء دیجیتال**
	محصول باید خدمات مرتبط با امضاء دیجیتال را مطابق با الگوریتم‌های زیر انجام بدهند: [انتخاب: • *الگوریتم امضای دیجیتال[1] با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با استاندارد FIPS PUB 186-3، «استاندارد امضای دیجیتال»* • *الگوریتم امضای دیجیتالRSA[2] با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با استاندارد FIPS PUB 186-2 یا FIPS PUB 186-3،«استاندارد امضای دیجیتال»* • *الگوریتم امضای دیجیتال منحنی بیضوی (ECDSA[3]) با کلید ۲۵۶ بیتی یا بیشتر مطابق با* o *FIPS PUB 186-3، «استاندارد امضای دیجیتال»* o *کارکرد امنیتی محصول باید منحنی‌های استاندارد[4] P-256، P384 و [گزینه: P251، نه سایر منحنی‌ها] (هم چنان که در FIPS PUB 186-3، «استاندارد امضای دیجیتال» تعریف شده است)] را پیاده‌سازی کند.*] **نکته کاربردی ۳۵:** نویسنده سند هدف امنیتی باید برای انجام امضای دیجیتال در قسمت «انتخاب» الگوریتم/الگوریتم‌هایی برگزیند، اگر نویسنده هدف امنیتی بیش از یک الگوریتم را انتخاب نماید، برای هر یک از این الگوریتم‌ها این الزام (شماره ۵۲ «مدیریت کلید رمزنگاری ۱») باید تکرار شوند. برای الگوریتم انتخاب‌شده، نویسنده هدف امنیتی باید گزینه‌ها/الزام‌های مناسب برای مشخص‌کردن پارامترهای آن، انجام دهد.
۷۱	**عملیات رمزنگاری ۱(۳) – درهم‌سازی**

[1] Digital Signature Algorithm (DSA)
[2] RSA Digital Signature Algorithm (rDSA)
[3] Elliptic Curve Digital Signature Algorithm (ECDSA)
[4] NIST curves

محصول باید درهم‌سازی را مطابق با الگوریتم رمزنگاری [انتخاب:*SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*] و اندازه‌ی خلاصه پیام[1] [انتخاب: *۱۶۰،۲۲۴، ۲۵۶، ۳۸۴ و ۵۱۲ بیت*] که مطابق با استاندارد FIPS 180-3، «استاندارد درهم‌ساز امن» باشد، انجام بدهند. **نکته کاربردی۳۶:** الگوریتم درهم‌سازی انتخاب‌شده باید متناسب با اندازه خلاصه پیام انتخاب‌شده باشد، به طور مثال اگر الگوریتم SHA-1 انتخاب‌شده است، تنها انتخاب، اندازه خلاصه پیام قابل قبول ۱۶۰ بیت خواهد بود. در نسخه‌های منتشرشده‌ی بعدی این پروفایل حفاظتی، احتمالاً SHA-1 الگوریتمی قابل تایید برای درهم‌سازی نخواهد بود.	
عملیات رمزنگاری۱(۴)- اصالت‌سنجی پیام	۷۲
محصول باید اصالت‌سنجی پیام مبتنی بر درهم‌سازی را مطابق یک الگوریتم رمزنگاری مشخص HMAC [انتخاب: SHA-1, SHA-256, SHA-384] و اندازه کلید [اختصاص: اندازه کلید (به بیت) مورد استفاده در HMAC] و اندازه‌های خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴] بیت که مطابق با استاندارد FIPS Pub 198-1، «کد اصالت‌سنجی پیام مبتنی بر کلید درهم‌سازی» و FIPS Pub 180-3، «استاندارد درهم‌سازی امن» باشد. **نکته کاربردی ۳۷:** در این نسخه از پروفایل حفاظتی، اجازه استفاده از رمزنگاری SHA-1 تنها برای TLS داده می‌شود. در نسخه‌های بعدی استفاده از آن کاملا حذف خواهد شد.	
پروتکل HTTPS ۱	۷۳
محصول مورد ارزیابی باید پروتکل HTTPS مطابق با RFC 2818 را اجرا کنند. **نکته کاربردی۳۸:** نویسنده هدف امنیتی باید اطلاعات کافی را فراهم آورد و مشخص کند که پیاده‌سازی این پروتکل، مطابق استانداردهای تعریف‌شده است. برای انجام این کار می‌توان عناصری را به این مؤلفه افزود یا اطلاعاتی را به خلاصه مشخصات محصول اضافه کرد.	
الزامات پروتکل HTTPS (۲)	۷۴

[1] Message Digest Sizes

محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS که در شماره ۷۷ الزام «الزامات پروتکلTLS/ احراز هویت ۱» اجرا کند.	
الزامات پروتکل IPSEC (۱)	۷۵
محصول باید ESP[1] پروتکل IPsec را به صورت تعریف‌شده توسط RFC4303 و با استفاده از الگوریتم‌های رمزنگاری AES-CBC-128، AES-CBC-256 (این دو الگوریتم در RFC 3602 مشخص‌شده‌اند)، [انتخاب: *هیچ الگوریتم دیگر، AES-GCM-128، AES-GCM-256 مشخص‌شده در RFC 4106*] و با استفاده از [انتخاب، حداقل یکی از موارد: *پروتکل IKE[2]v1 به صورت تعریف‌شده در RFC های2407، 2408، 2409، 4109 و [انتخاب: هیچ RFC دیگر برای توابع درهم‌سازی، RFC 4868 برای توابع درهم‌سازی]؛ پروتکل IKEv2 تعریف‌شده در RFC های 5996، 4307 و [انتخاب: هیچ RFC دیگر برای توابع درهم‌سازی، RFC 4868 برای توابع درهم‌سازی*]] پیاده‌سازی نماید. **نکته کاربردی ۳۹:** در اولین انتخاب می‌توان الگوریتم‌های رمزنگاری بیشتری را برگزید. در دومین انتخاب باید مشخص گردد که از پروتکل IKEv1 پشتیبانی می‌گردد یا IKEv2. برای پروتکل IKEv1، در صورتی که پیاده‌سازی IKE مطابق با RFC 2409 باشد و اضافات و تغییرات در RFC 4109 توصیف‌شده باشد الزام تفسیر می‌گردد. RFC 4868 توابع درهم‌سازی بیشتری را برای استفاده IKEv1 و IKEv2 معرفی می‌نماید.	
الزامات پروتکل IPSEC (۲)	۷۶
محصول باید این اطمینان را بدهند که تبادلات فاز ۱ IKEv1 تنها در مد اصلی استفاده می‌گردد.	
الزامات پروتکل IPSEC (۳)	۷۷
محصول باید اطمینان دهد که طول عمر SA مربوط به IKEv1 قادر است برای فاز ۱ SA به ۲۴ ساعت محدود گردد و برای فاز ۲ SA به ۸ ساعت محدود گردد. **نکته کاربردی ۴۰:** الزام بالا می‌تواند توسط طول عمری که توسط سرپرست امنیتی قابل تنظیم است (با الزامات کلاس مدیریت مناسب، یا دستوراتی که در سند شرح محصول	

[1] Encapsulating Security Payload
[2] Internet Key Exchange

ذکرشده است) انجام شود و یا توسط «کدنویسی سخت» که پیاده‌سازی را محدود می‌نماید.	
الزامات پروتکل IPSEC (۴)	۷۸
محصول باید اطمینان دهد که طول عمر SA مربوط به IKEv1 قادر است برای فاز ۲ SA به [اختصاص: **عددی بین ۱۰۰-۲۰۰**] مگابایت، محدود گردد. **نکته کاربردی ۴۱:** الزام بالا می‌تواند توسط طول عمری که توسط سرپرست امنیتی قابل تنظیم است (با الزامات کلاس مدیریت امنیت، یا دستورات ذکرشده در سند شرح محصول) انجام شود و یا توسط «کدنویسی سخت» که پیاده‌سازی را محدود می‌نماید. نویسنده هدف امنیتی، مقدار عددی را در بازه‌ی مشخص‌شده تعیین می‌نماید. به طور کلی، دستورالعمل‌ها برای تنظیم پارامترهای پیاده‌سازی، همچون طول عمر SA، باید توسط الزامات کلاس مدیریت مشخص گردند و در سند شرح محصول ذکرشده باشند.	
الزامات پروتکل IPSEC (۵)	۷۹
محصول باید اطمینان دهند که تمام پروتکل‌های IKE گروه‌های DH، ۱۴(۲۰۴۸ بیت MODP) و [انتخاب: *۲۴(۲۰۴۸ بیت MODP با ۲۵۶ بیت POS*، *۱۹ (۲۵۶ بیت تصادفی ECP)*، *۲۰ (۳۸۴ بیت تصادفی ECP)*، *[اختصاص: **دیگر گروه‌های DH که توسط هدف ارزیابی پیاده‌سازی شده‌اند**]*، *هیچ گروه دیگر DH*] را پیاده‌سازی می‌نمایند. **نکته کاربردی ۴۲:** این مؤلفه، هدف ارزیابی را ملزم به پشتیبانی از گروه DH 14 می‌نماید. در صورت پشتیبانی از دیگر گروه‌ها، این گروه‌ها باید انتخاب گردند یا در قسمت «اختصاص» بالا مشخص گردند، در غیر این صورت «هیچ گروه دیگر DH» انتخاب می‌گردد. این الزام به تبادلات IKEv1و (در صورت پیاده‌سازی شدن) به IKEv2 اعمال می‌گردد.	
الزامات پروتکل IPSEC (۶)	۸۰
محصول باید اطمینان دهند که تمام پروتکل‌های IKE با استفاده از الگوریتم [انتخاب: *DSA، rDSA، ECDSA*] احراز هویت همتا را پیاده‌سازی می‌نمایند. **نکته کاربردی ۴۳:** الگوریتم انتخاب‌شده باید با انتخاب صورت گرفته در الزام شماره ۵۵ «عملیات رمزنگاری ۱(۲)- امضاء دیجیتال» در ارتباط باشد.	

<table dir="rtl">
<tr><td>۸۱</td><td>الزامات پروتکل IPSEC (۷)</td></tr>
<tr><td colspan="2">محصول باید استفاده‌ی کلیدهای از قبل به اشتراک گذاشته‌شده را (همان‌طور که در RFC ها اشاره‌شده است) برای استفاده در احراز هویت اتصالات خود IPsec پشتیبانی نمایند.</td></tr>
<tr><td>۸۲</td><td>الزامات پروتکل IPSEC (۸)</td></tr>
<tr><td colspan="2">محصول باید موارد زیر را پشتیبانی نمایند:
• کلیدهای از پیش به اشتراک گذارده شده، باید قادر باشند از هر ترکیبی از حروف بزرگ، حروف کوچک، اعداد و کاراکترهای خاص: [انتخاب: "!"، "@"، "#"، "$"، "٪"، "^"، "&"، "*"، ")"، "("، [اختصاص: دیگر کاراکترها]] تشکیل گردند.
• کلیدهای از پیش به اشتراک گذاشته‌شده ۲۲ کاراکتر و [انتخاب: [اختصاص: دیگر طول کلیدهایی که پشتیبانی می‌شود]، بدون دیگر اندازه-های کلید] باشند.
نکته کاربردی ۴۴:
نویسنده هدف امنیتی باید کاراکترهای خاصی را انتخاب نماید که توسط هدف ارزیابی قابل پشتیبانی باشد. ممکن است با استفاده از قابلیتی که در قسمت «اختصاص» ارائه‌شده، این اختیار به نویسنده داده‌شده است تا بتواند کاراکترهای بیشتری را تعریف نماید.
برای طول کلیدهای از پیش به اشتراک گذاشته‌شده، طول کلید معمولی (۲۲ کاراکتر) برای کمک به ترویج قابلیت همکاری نیاز است. اگر طول کلیدهای دیگر پشتیبانی می‌شود باید در قسمت «اختصاص» لیست گردد، هم‌چنین در این قسمت می‌توان یک محدوده را برای طول کلید مشخص نمود (به طور مثال طول کلید از ۵ تا ۵۵ کاراکتر).</td></tr>
<tr><td>۸۳</td><td>تولید بیت تصادفی ۱</td></tr>
<tr><td colspan="2">محصول مورد ارزیابی باید خدمات تولید بیت تصادفی را بر اساس ISO/IEC 18031:2011 و با استفاده از [انتخاب: Hash_DRBG، HMAC_DRBG، CTR_DRBG (AES)] ارائه دهد.</td></tr>
<tr><td>۸۴</td><td>تولید بیت تصادفی ۲</td></tr>
<tr><td colspan="2">RBG قطعی باید دست‌کم توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی را از [انتخاب: [اختصاص: تعداد مشخص] منبع نویز مبتنی بر نرم‌افزار، [اختصاص: تعداد مشخص] منبع نویز مبتنی بر سخت‌افزار] گردآوری کند. این آنتروپی باید دست‌کم [انتخاب: ۱۲۸ بیت، ۱۹۲ بیت، ۲۵۶ بیت] و</td></tr>
</table>

حداقل معادل بالاترین قدرت امنیتی کلیدها و درهم‌سازهای تولیدشده مورداشاره در بخش «جدول قدرت امنیتی توابع درهم‌ساز» ISO/IEC 18031:2011 باشد. **نکته کاربردی ۴۵:** در مورد نخستین عبارت انتخاب در «تولید بیت تصادفی ۲»، هدف امنیتی باید حداقل به یکی از انواع منابع نویز اشاره کند. اگر محصول مورد ارزیابی شامل چند منبع نویز از یک نوع باشد، نویسنده هدف امنیتی عبارت اختصاص را با تعداد مناسبی از هر یک از انواع منابع پر می‌کند (مثلاً دو منبع نویز مبتنی بر نرم‌افزار و یک منبع نویز مبتنی بر سخت‌افزار). مستندات و آزمون‌های مورداشاره در فعالیت‌های ارزیابی، تمام منابع مورداشاره در هدف امنیتی را پوشش می‌دهند. سند ISO/IEC 18031:2011 شامل سه روش مختلف تولید اعداد تصادفی است که هر یک از آن‌ها به عناصر اولیه فرایند رمزنگاری (توابع درهم‌ساز و مجموعه‌های رمز) بستگی دارد. نویسنده هدف امنیتی، تابع مورداستفاده را انتخاب خواهد کرد و عناصر اولیه فرایند رمزنگاری را تعیین خواهد نمود. بااینکه تمام توابع درهم‌ساز تعیین‌شده (SHA-1,SHA-224, SHA-256, SHA-384, SHA-512) را می‌توان در Hash_DRBG یا HMAC_DRBG مورداستفاده قرار داد، تنها اجازه استفاده از موارد مبتنی بر AES در CTR_DRBG وجود دارد.	
الزامات پروتکل SSH(۱)	۸۵
محصول باید پروتکل SSH مطابق با RFC های 4251، 4252، 4253، 4254 و [انتخاب: RFC های 5647، 5656، 6187، 6668، هیچ RFC دیگری] را پیاده‌سازی نماید. **نکته کاربردی۴۶:** نویسنده هدف امنیتی انتخاب می‌کند که مطابقت با کدام یک از RFC های اضافی اعلام شود. توجه شود که این RFC ها باید با RFC های موارد بعدی این جزء نیز مطابقت داشته باشند (مثلاً، مجاز بودن الگوریتم‌های رمزنگاری). RFC4253 مشخص می‌کند که الگوریتم‌های رمزنگاری خاصی **الزامی** هستند. در نتیجه، این الگوریتم‌ها باید در پیاده‌سازی پشتیبانی شوند، نه این که صرفاً امکان استفاده از آن‌ها وجود داشته باشد. اطمینان حاصل کردن از این که الگوریتم‌های الزامی، ولی ذکرنشده در موارد بعدی این جزء، پیاده‌سازی می‌شوند، خارج از میدان فعالیت تضمینی برای این الزام است.	
الزامات پروتکل SSH(۲)	۸۶
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، روش‌های احراز هویت زیر مطابق با آنچه که در RFC4252 توضیح داده‌شده است،	

پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، احراز هویت مبتنی بر کلمه عبور.	
الزامات پروتکل SSH (۳)	۸۷
همان طور که در RFC4253 توضیح داده‌شده است، محصول باید اطمینان حاصل نماید که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک ارتباطات انتقال SSH کنار گذاشته شوند. **نکته کاربردی ۴۷:** RFC4253 امکان پذیرش «بسته‌های بزرگ» را فراهم می‌کند، با این اخطار که بسته‌ها باید «طول مناسبی» داشته باشند یا اینکه کنار گذاشته می‌شوند. توصیه می‌شود این اختصاص توسط نویسنده هدف امنیتی با در نظر گرفتن بیشترین اندازه بسته که قابل‌پذیرش است پر شود تا به این وسیله «طول مناسب» برای محصول تعریف شود.	
الزامات پروتکل SSH (۴)	۸۸
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری زیر استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند: aes128-cb,aes256-cbc,[انتخاب:AEAD_AES_128_GCM, AEAD_AES_256_GCM, یا هیچ الگوریتم دیگری] **نکته کاربردی۴۸:** RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GC را در SSH مشخص می‌کند. همانطور که در RFC 5647 آمده استAEAD_AES_128_GCM وAEAD_AES_256_GCM تنها زمانی می‌توانند به عنوان الگوریتم های MAC انتخاب شوند که الگوریتم متناظر برای رمزنگاری انتخاب‌شده باشد. در بخش اختصاص، نویسنده هدف امنیتی می‌تواند الگوریتم AES-GCM را انتخاب کند یا اگر الگوریتم AES-GCM قابل پشتیبانی نبود، «هیچ الگوریتم دیگری» را انتخاب کند. اگر AES-GSM انتخاب شود باید «عملیات رمزنگاری» متناظر هم در سند هدف امنیتی آورده شود.	
الزامات پروتکل SSH(۵)	۸۹
محصول باید اطمینان حاصل نماید که پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: ssh-rsa, ecdsa-sha2-nistp256] و [انتخاب: ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, هیچ الگوریتم کلید عمومی دیگری] به عنوان الگوریتم‌های	

کلید عمومی خودش استفاده می‌کند و سایر الگوریتم‌های کلید عمومی رد می‌شوند. **نکته کاربردی۴۹:** در پیاده‌سازی‌هایی که تنها از ssh-rsa استفاده می‌شود، استحکام امنیتی ۱۱۲ بیتی که در تولید امضای دیجیتال به منظور احراز هویت SSH ای که درNIST SP 800-131A پیشنهادشده حاصل نمی‌شود. اگر x509v3-ecdsasha2-nistp256 یا x509v3-ecdsa-sha2-nistp384انتخاب شوند، لیست CA های معتبر باید از «الزامات پروتکل SSH Client (۸)» انتخاب شود.	
۹۰	**الزامات پروتکل SSH (۶)**
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512، هیچ الگوریتم MAC دیگر] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند. **نکته کاربردی۵۰:** RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GC را در SSH مشخص می‌کند. همانطور که در RFC 5647 آمده است AEAD_AES_128_GCM وAEAD_AES_256_GCM تنها زمانی می‌توانند به عنوان الگوریتم های MAC انتخاب شوند که الگوریتم متناظر برای رمزنگاری انتخاب‌شده باشد. RFC 6668 استفاده از الگوریتم sha2 را در SSH مشخص می‌کند.	
۹۱	**الزامات پروتکل SSH (۷)**
محصول باید اطمینان حاصل نماید که [انتخاب: ecdh-sha2-nistp256,diffie-hellman-group14-sha1] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.	
۹۲	**الزامات پروتکلTLS/ احراز هویت ۱**
محصول باید [انتخاب: TLS 1.2 (RFC5246)، TLS1.1 (RFC4346)] را با پشتیبانی از مجموعه‌های رمز زیر، پیاده‌سازی نماید: • مجموعه‌های رمز اجباری: o TLS_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268	

- [انتخاب: مجموعه‌های رمز اختیاری:
  - [TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
  - TLS_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5246
  - TLS_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
  - TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256مطابق با RFC 5246
  - TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
  - هیچ مجموعه رمز دیگری]].

نکته کاربردی۵۱:

مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدود شده‌اند. نویسنده هدف امنیتی باید از بین مجموعه‌های رمز اختیاری

مورد پشتیبانی، انتخاب نماید. در صورتی که هیچ مجموعه رمز اختیاری وجود نداشته باشد، هیچ انتخابی ننماید. توجه شود که به منظور اطمینان از مطابقت با RFC5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.

۹ پیوست دو: انواع معماری و الزامات اضافی

۱,۹ انواع معماری برای کنترل دسترسی با استفاده از انواع تکنولوژی

با توجه به انواع مختلف کنترل دسترسی‌ها که می‌توانند در محصول مورد استفاده قرار بگیرند در این پروفایل حفاظتی آمده است. این مولفه‌ها اختیاری نیستند آن‌ها باید با توجه به نوع حفاظت از داده‌ها به‌طور واضح تکمیل شوند.

- **کنترل دسترسی مبتنی بر میزبان**

کنترل دسترسی مبتنی بر میزبان برای این‌که موجودیت فعال به چه سیستم و کارکرد خاص دسترسی داشته باشد مورد استفاده قرار می‌گیرد. هدف از این تکنولوژی جلوگیری موجودیت فعال از عملیات غیرمجاز و اجرای مخرب و نامناسب در اجرای نرم افزار یا تغییر پیکربندی است. این نوع کنترل دسترسی رفتارهای زیر را دارند ولی تنها محدود به این رفتارها نیستند:

- ✓ **دسترسی به برنامه:** اجرای یک برنامه که کارکرد سازمانی قانونی را ارائه نمی‌کند، حذف یک برنامه که کارکرد سازمانی قانونی را ارائه می‌کند، یا خاتمه به اجرای برنامه یا پروسه که کارکرد سازمانی را ارائه می‌نماید (به عنوان مثال، ممیزی)
- ✓ **دسترسی به فایل:** ایجاد یک فایل در مکان غیر معتبر، خواندن یک فایل شامل داده‌های موجودیت فعال است که اجازه دسترسی نباید داشته شود، ویرایش یا حذف یک فایل که محتوی اطلاعات مهم است یا بر روی رفتار برنامه قانونی تاثیر می‌گذارد، یا تغییر مجوزهای فایل برای اجازه دسترسی به موجودیت‌های غیرفعال ناامن
- ✓ **پیکربندی میزبان:** خواندن، تغییر یا حذف مقادیری که کارکرد میزبان را تعریف می‌کند مانند رجیستری ویندوز که تلاش برای تغییر رفتار قانونی یک برنامه یا کل سیستم دارد.

شماره الزام	نام الزام
۹۳	**خط‌مشی کنترل دسترسی ۱**

محصول باید بر روی کنترل دسترسی خط‌مشی امنیتی بتواند موارد زیر را اعمال نماید: [

- موجودیت‌های فعال: زیرمجموعه‌ای از کاربران که داده‌های سازمانی ذخیره می‌کنند، [اختصاص: دیگر موجودیت‌های فعال]
- موجودیت‌های غیرفعال: برنامه‌ها، فایل‌ها، پیکربندی میزبان، توابع احراز هویت [اختصاص: دیگر موجودیت‌های غیرفعال]
- عملیات: توانایی ایجاد، خواندن، تغییر، اجرا، حذف، خاتمه یا تغییر مجوز موجودیت غیرفعال و توانایی استفاده از توابع احراز هویت، [اختصاص: دیگر عملیات‌ها]]

نکته کاربردی ۵۲:

موجودیت فعال، موجودیت غیرفعال و عملیات باید در نقشه سازمانی توسط مدیر خط‌مشی سازمان تعریف‌شده باشد.

شماره الزام	نام الزام
۹۴	**عملیات کنترل دسترسی ۱**

محصول باید [خط‌مشی کنترل دسترسی] براساس [تمام عملیات‌های بین موجودیت‌های غیرفعال و فعال که در جدول زیر تعریف‌شده] به موجودیت‌های غیرفعال اعمال نماید.

موجودیت فعال	موجودیت غیرفعال	عملیات
کاربر	فرایندها (پروسه‌ها)	اجرا| حذف| خاتمه
		تغییر مجوزها
	فایل‌ها	ایجاد | خواندن | ویرایش | حذف
		تغییر مجوزها
	پیکربندی میزبان	خواندن | ویرایش | حذف
	توابع احراز هویت	ورود به سیستم

شماره الزام	نام الزام
۹۵	**عملیات کنترل دسترسی ۲**

محصول باید قوانین زیر را اجرا نمایند تا عملیات بین موجودیت فعال کنترل‌شده و موجودیت غیرفعال کنترل‌شده را مجاز نمایند: [اختصاص: انواع قوانینی

که از سامانه مدیریت خط‌مشی مجاز دریافت نموده است]	
۹۶	**عملیات کنترل دسترسی ۳**
محصول باید به‌طور واضح و مشخص براساس قوانین زیر، دسترسی مجاز از موجودیت‌های فعال به موجودیت‌های غیرفعال داشته باشد: [اختصاص: **تعریف قوانین بیشتر**.] **نکته کاربردی۵۳:** نویسنده سند هدف امنیتی باید قوانین دیگری که قوانین سامانه کنترل دسترسی نادیده می‌گیرد را به‌طور واضح بیان نماید. به عنوان مثال، قوانین اضافی ممکن است اجازه دهد که مالک موجودیت غیرفعال قادر به اعمال هر گونه عملیات بر روی موجودیت غیرفعال باشد.	
۹۷	**عملیات کنترل دسترسی ۴**
محصول باید براساس قوانین زیر از دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال جلوگیری می‌کند: [اختصاص: **تعریف قوانین بیشتر**.] **نکته کاربردی ۵۴:** نویسنده سند هدف امنیتی باید موجودیت‌های غیرفعال مشخصی که توسط فرایند ممانعت واضح[۱] محافظت‌شده هستند را بیان نماید. فرایند ممانعت باید مستقل از هر نوع خط‌مشی مورد استفاده توسط محصول پیاده‌سازی شده باشد.	
۹۸	**خط‌مشی کنترل دسترسی ۱ (۲)**
محصول باید [خط‌مشی کنترل دسترسی حفاظت از خود] را بر روی موارد زیر را اعمال نماید:[• موجودیت‌های فعال: زیرمجموعه‌ای از کاربران که داده‌های سازمانی ذخیره می‌کنند، [اختصاص: دیگر موجودیت‌های فعال] • موجودیت‌های غیرفعال: برنامه‌ها، فایل‌ها، مقادیر پیکربندی که شامل داده‌های محصول می‌باشد، [اختصاص: دیگر موجودیت‌های غیرفعال] • عملیات: توانایی ایجاد، خواندن، تغییر، اجرا، حذف، خاتمه یا تغییر مجوز موجودیت غیرفعال، [اختصاص: دیگر عملیات‌ها]] **نکته کاربردی ۵۵:** هدف از این الزام، محافظت از خود محصول در برابر تغییرات یا خاتمه هر خط‌مشی غیرمجاز می‌باشد.	

[۱] Explicit denial process

۹۹	**عملیات کنترل دسترسی ۱ (۲)**
	محصول باید [خط‌مشی کنترل دسترسی حفاظت از خود] را براساس [تمام عملیات‌های بین موجودیت‌های غیرفعال و فعال که طبق برخی از مشخصه-های سازمانی هستند] به موجودیت‌های غیرفعال اعمال نماید. **نکته کاربردی ۵۶:** محصول نباید مشخصه‌هایی را برای موجودیت فعال و غیرفعال تعریف نماید. بلکه انتظار می‌رود، به مشخصه‌های موجودیت فعال و غیرفعال داده‌های دریافت شده اتکا نماید.
۱۰۰	**عملیات کنترل دسترسی ۲ (۲)**
	محصول باید قوانین زیر را اجرا نمایند تا عملیات بین موجودیت فعال کنترل‌شده و موجودیت غیرفعال کنترل‌شده را مجاز نمایند: [محصول به عملیات درخواست شده در برابر موجودیت‌های غیرفعالی که محافظت‌شده هستند، مجوز نمی‌دهد مگر آنکه موجودیت فعالی که اقدام نموده مسئولیت نصب محصول و پیکربندی اولیه آن را برعهده داشته است.]
۱۰۱	**عملیات کنترل دسترسی ۳ (۲)**
	محصول باید براساس قوانین زیر، دسترسی مجاز از موجودیت‌های فعال به موجودیت‌های غیرفعال داشته باشند: [هیچ**]**
۱۰۲	**عملیات کنترل دسترسی ۴ (۲)**
	محصول باید براساس قوانین زیر از دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال جلوگیری کند: [هیچ**]**

- **کنترل دسترسی مبتنی بر وب**

سازوکار کنترل دسترسی مبتنی بر وب برای تعیین منابع برخطی که موجودیت فعال بر روی یک سیستم خاص دسترسی داشته باشد بکار گرفته می‌شود. هدف از این تکنولوژی، جلوگیری موجودیت فعال از تعامل با محتویات برخط غیرمجازی که درون یک برنامه کاربردی دیگر هستند. به عنوان مثال، ممکن است یک سازمان از یک برنامه چندرسانه‌ای برای نمایش نشست‌های آموزشی شرکت‌کنندگان راه دور استفاده نماید درحالی-که به همان برنامه اجازه نمایش رویدادهای ورزشی را ندهد. معمولا این نوع کنترل دسترسی‌ها ویژگی‌های زیر را داشته باشند ولی محدود به این-ها نمی‌باشند:

- ✓ دسترسی به URL ها: دسترسی به محتویات برخط شناخته‌شده توسط یک URL که ممکن است شامل محتویات نامناسب و یا مخرب باشد.
- ✓ دسترسی به اسکریپت‌های قابل اجرا: اجرای یک اسکریپت از قبیل JSP، یا ActiveX که درون یک صفحه وب قرار دارند یا کنترل (فعال/غیر فعال‌سازی) افراد برای اجرای این اسکریپت‌ها
- ✓ دسترسی به فرم‌ها: بارگذاری یک فایل یا داده‌ها در یک صفحه وب از طریق عملیات HTTP(GET, POST) که هدف قانونی سازمان را ارائه نمی‌کنند از قبیل سایت یک شبکه اجتماعی

<table dir="rtl">
<tr><th>شماره الزام</th><th>نام الزام</th></tr>
<tr><td>۱۰۳</td><td>خط‌مشی کنترل دسترسی ۱</td></tr>
<tr><td colspan="2">محصول باید بر روی کنترل دسترسی خط‌مشی امنیتی بتواند موارد زیر را اعمال نماید: [
• موجودیت‌های فعال: زیرمجموعه‌ای از کاربران که داده‌های سازمانی ذخیره می‌کنند و
• موجودیت‌های غیرفعال: URL ها، فایل‌ها، اسکریپت‌های قابل اجرا، فرم‌ها و
• عملیات: دسترسی، بارگذاری، بارگیری (دانلود)، اجرا، فعال‌سازی، غیر فعال‌سازی و عملیات] HTTP</td></tr>
<tr><td>۱۰۴</td><td>عملیات کنترل دسترسی ۱</td></tr>
<tr><td colspan="2">محصول باید [خط‌مشی کنترل دسترسی] براساس [تمام عملیات‌های بین موجودیت‌های غیرفعال و کاربران که در جدول زیر تعریف‌شده] به موجودیت-های غیرفعال اعمال نماید.
<table dir="rtl">
<tr><th>موجودیت فعال</th><th>موجودیت غیرفعال</th><th>عملیات</th></tr>
<tr><td rowspan="5">کاربر</td><td>URL ها</td><td>دسترسی از طریق عملیات HTTP</td></tr>
<tr><td>فایل‌ها</td><td>باز کردن | دانلود</td></tr>
<tr><td rowspan="2">اسکریپت‌های قابل اجرا</td><td>اجرا کردن</td></tr>
<tr><td>فعال/ غیر فعال‌سازی</td></tr>
<tr><td>فرم‌ها</td><td>HTTP GET | HTTP POST</td></tr>
</table>
</td></tr>
<tr><td>۱۰۵</td><td>عملیات کنترل دسترسی ۲</td></tr>
<tr><td colspan="2">محصول باید قوانین زیر را اجرا نماید تا عملیات بین موجودیت فعال کنترل‌شده و موجودیت غیرفعال کنترل‌شده را مجاز نمایند: [اختصاص: انواع قوانینی که از سامانه مدیریت خط‌مشی مجاز دریافت نموده است]</td></tr>
</table>

۱۰۶	**عملیات کنترل دسترسی ۳**
	محصول باید به‌طور واضح و مشخص براساس قوانین زیر، دسترسی مجاز از موجودیت‌های فعال به موجودیت‌های غیرفعال داشته باشد: [اختصاص: **تعریف قوانین بیشتر**.] **نکته کاربردی ۵۷:** هدف از این الزام این است، به‌طور مجاز و واضح در شرایطی که هرگز کنترل دسترسی بکار گرفته نمی‌شود، پروسه اعمال قوانین نادیده گرفته شود. برای مثال، پشتیبانی از دسترسی گمنامی[۱] است، از قبیل اجازه براساس آدرس مبداء (درخواست‌های داخلی نیاز به احراز هویت ندارند)، در صورتی که محتویات وب در دامنه وب سازمان قرارگرفته باشد، تمامی کاربران محصول اجازه خواندن داده‌ها را دارند مگر این‌که نیاز به احراز هویت داشته باشند.
۱۰۷	**عملیات کنترل دسترسی ۴**
	محصول باید براساس قوانین تکمیلی زیر از دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال به‌طور واضح جلوگیری کند: [اختصاص: **تعریف قوانین بیشتر**.] **نکته کاربردی ۵۸:** نویسنده سند هدف امنیتی باید موجودیت‌های غیرفعال مشخصی که توسط فرایند ممانعت واضح[۲] محافظت‌شده هستند را بیان نماید. فرایند ممانعت باید مستقل از هر نوع خط‌مشی مورد استفاده توسط محصول پیاده‌سازی شده باشد.

۱ Anonymous

۲ Explicit denial process

- **کنترل دسترسی مبتنی بر جلوگیری از نشت داده‌ها**

کنترل دسترسی جلوگیری از نشت داده‌ها برای کاهش ریسک به مخاطره افتادن داده‌ها بین دامنه‌های امنیتی مختلف مورد استفاده قرار می‌گیرد. محصول کنترل دسترسی جلوگیری از نشت داده‌ها، باید قادر به شناسایی داده‌های مهم و حساس باشد هنگامی‌که به دامنه خارجی انتقال داده می‌شوند و از این عمل ممانعت نماید. ویژگی‌های مهمی که این نوع کنترل دسترسی‌ها دارند به شرح زیر می‌باشد:

- ✓ افشاء spool چاپگر: چاپ داده‌های حساس با قبول آن‌ها در spool چاپگر، بنابراین به‌طور فیزیکی می‌توان spool را به مکان غیرمجاز منتقل نمود.
- ✓ افشاء پروتکل لایه کاربردی: انتقال داده‌های حساس از طریق برنامه کاربردی از قبیل ارسال ایمیل که شامل آن داده‌ها است و یا بارگذاری یک فایل از طریق فرم تحت وب که شامل داده‌های حساس می‌باشد.
- ✓ افشاء فایل: نمایش یک فایل که شامل داده‌های حساس است که موجودیت فعال مجاز به نمایش یا انتقال، کپی آن‌ها به دامنه کم امن از قبیل دیگر درایوها نمی‌باشد.
- ✓ افشاء حافظه موقت[۱]: کپی داده‌های حساس و مهم درون یک فایل باز، ممکن است این فایل در دامنه کم امنی قرارگرفته باشد.
- ✓ افشاء دستگاه‌های قابل حمل: نوشتن یک فایل محتوی داده‌های حساس به یک دستگاه قابل حمل، در این صورت امکان دارد این دستگاه به طور فیزیکی به مکان ناامن و غیرمجاز برده شود.

لازم به ذکر است که این نوع کنترل دسترسی محیط کاملا امنی را در برابر عملیات مخرب داخلی فراهم نمی‌کند. بلکه تهدیدات احتمالی را کاهش می‌دهد.

شماره الزام	نام الزام
۱۰۸	**خط‌مشی کنترل دسترسی ۱**

۱ Clipboard

محصول باید بر روی کنترل دسترسی خط‌مشی امنیتی بتواند موارد زیر را اعمال نماید: [

- موجودیت‌های فعال: زیرمجموعه‌ای از کاربران که داده‌های سازمانی ذخیره می‌کنند و
- موجودیت‌های غیرفعال: مکان‌های محلی و راه دوری که امکان دریافت و ذخیره یا عملیات دیگر بر روی داده‌های حساس و مهم دارند و
- عملیات: دسترسی، قبول کردن[۱]، انتقال، نمایش، کپی، چسباندن، نوشتن به و
- مشخصه‌ها: رشته‌ای از داده‌های حساس و فایل‌ها یا مخازنی که شامل چنین داده‌هایی هستند (به عنوان مثال PII[۲])]

۱۰۹	**عملیات کنترل دسترسی ۱**

محصول باید [خط‌مشی کنترل دسترسی] براساس [تمام عملیات‌های بین موجودیت‌های غیرفعال و کاربران که در جدول زیر تعریف‌شده] به موجودیت‌های غیرفعال اعمال نماید.

موجودیت فعال	موجودیت غیرفعال	عملیات
کاربر	spool چاپگر	قبول (انتقال به دامنه امنیتی بیرونی)
	پروتکل لایه کاربردی	ارسال (انتقال به دامنه امنیتی بیرونی)
	فایل	نمایش | انتقال | کپی (به دامنه‌های دیگر)
	حافظه موقت	کپی/چسباندن (به مکان دیگر)
	دستگاه قابل حمل	نوشتن در (دامنه بیرونی امن)

[۱] Submit

[۲] Personal Identifilable Information

۱۱۰	**عملیات کنترل دسترسی ۲**

محصول باید قوانین زیر را اجرا نماید تا عملیات بین موجودیت فعال کنترل‌شده و موجودیت غیرفعال کنترل‌شده را مجاز نمایند: [انواع قوانینی که از سامانه مدیریت خط‌مشی مجاز دریافت نموده است:

- مشخصه‌های داده‌های محیطی، ممکن است با مشخصه‌های امنیتی مانند اطلاعات حساس علامت‌گذاری شوند یا اجازه افشاء داده نشود (مانند PII، داده‌های دسته‌بندی شده) و
- موجودیت‌های غیرفعالی که شامل این نوع داده‌ها هستند باید از انتقال سیستم به مکان دیگر ممانعت شوند مگر این‌که مقصد مورد نظر، مکان امنی باشد و
- سازوکار انتقال از سیستم، به دستگاه‌های منطقی دیگر، چاپ کردن و کپی به حافظه موقت باید به‌طور نظام‌مند مشخص‌شده باشد].

نکته کاربردی ۵۹:

نویسنده سند هدف امنیتی باید انواع و مقادیر داده‌ها را که محصول آن‌ها را مهم و حساس در نظر می‌گیرد، مشخص نماید.

۱۱۱	**عملیات کنترل دسترسی ۳**

محصول باید به‌طور واضح و مشخص براساس قوانین زیر، دسترسی مجاز از موجودیت‌های فعال به موجودیت‌های غیرفعال داشته باشد:

[در صورتی که موجودیت غیرفعال در حال انتقال به یک مقصد مانند گیرنده ایمیل یا درایو منطقی و یا به مکان داخلی سازمان باشد که به عنوان مقصد امن مشخص‌شده‌اند، به عملیات اجازه داده شود].

نکته کاربردی ۶۰:

نویسنده سند هدف امنیتی باید الزاماتی را تعریف نماید که محصول می‌تواند یک دستگاه منطقی را به عنوان مکان امن نشانه‌گذاری[۱] تعیین کند.

۱۱۲	**عملیات کنترل دسترسی ۴**

محصول باید براساس قوانین تکمیلی زیر از دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال به‌طور واضح جلوگیری کند:

[اختصاص: **تعریف قوانین بیشتر**.]

نکته کاربردی ۶۱:

[۱] Flagged as trusted

نویسنده سند هدف امنیتی باید موجودیت‌های غیرفعال مشخصی که توسط فرایند ممانعت واضح[۱] محافظت‌شده هستند را بیان نماید. فرایند ممانعت باید مستقل از هر نوع خط‌مشی مورد استفاده توسط محصول پیاده‌سازی شده باشد.

۲٫۹ مؤلفه‌های خود پایشی[۲] محصول

محصول کنترل دسترسی مبتنی بر میزبان ممکن است که قابلیت اضافی در برابر خاتمه خود توسط کاربر غیرمجاز توسط پایش خود و اطمینان‌سازی از کارکردهای خود فراهم آورد. در این صورت باید نویسنده سند هدف امنیتی باید الزام زیر را نیز تکمیل نماید:

شماره الزام	نام الزام
۱۱۳	**حفظ وضعیت امن در زمان شکست ۱**
محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند: [اختصاص: لیستی از مؤلفه‌های محصول و وضعیت‌های کارکردهای غیرقانونی ممکن] **نکته کاربردی ۶۲:** در حفظ وضعیت امن، محصول باید به‌طور خودکار شکست را برطرف نماید و یا به وضعیت ممانعت پیش‌فرض[۳] برود و اعلان نماید که باید عملیات اصلاحی به‌طور دستی انجام بگیرد.	

[۱] Explicit denial process
[۲] Self-Monitoring
[۳] Default-deny state